

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

Any NRC personnel and any personnel from NRC contractor organizations may submit an Environment Change Request (ECR). ECRs propose additions, deletions, or modifications to the current environment¹.

3. REFERENCE PUBLICATIONS

The following publications contain related information:

- *SDLCM Methodology Handbook*
- SDLCM Methodology Form F-1601, Environment Change Request Form
- SDLCM Methodology Procedure P-2501, Configuration Control Board
- NRC Technical Reference Model, NRC/OCIO

4. PROCEDURE

4.1 Data Flow Diagram

The Environment Change procedure has the five major steps identified in the data flow diagram shown in Figure 1601-1.

4.2 Entry Criteria

This section identifies the inputs and triggers.

The following input is necessary to begin this procedure:

- A recognized need for an addition, deletion, or modification to the NRC environment

Any of the following events may trigger this procedure:

- A failure of the environment to support a functional requirement
- An opportunity for process improvement
- The introduction of new technology
- Cessation of vendor support

¹ In a future revision to this procedure, the phrase "current environment" will be changed to "baselined operational environment."

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

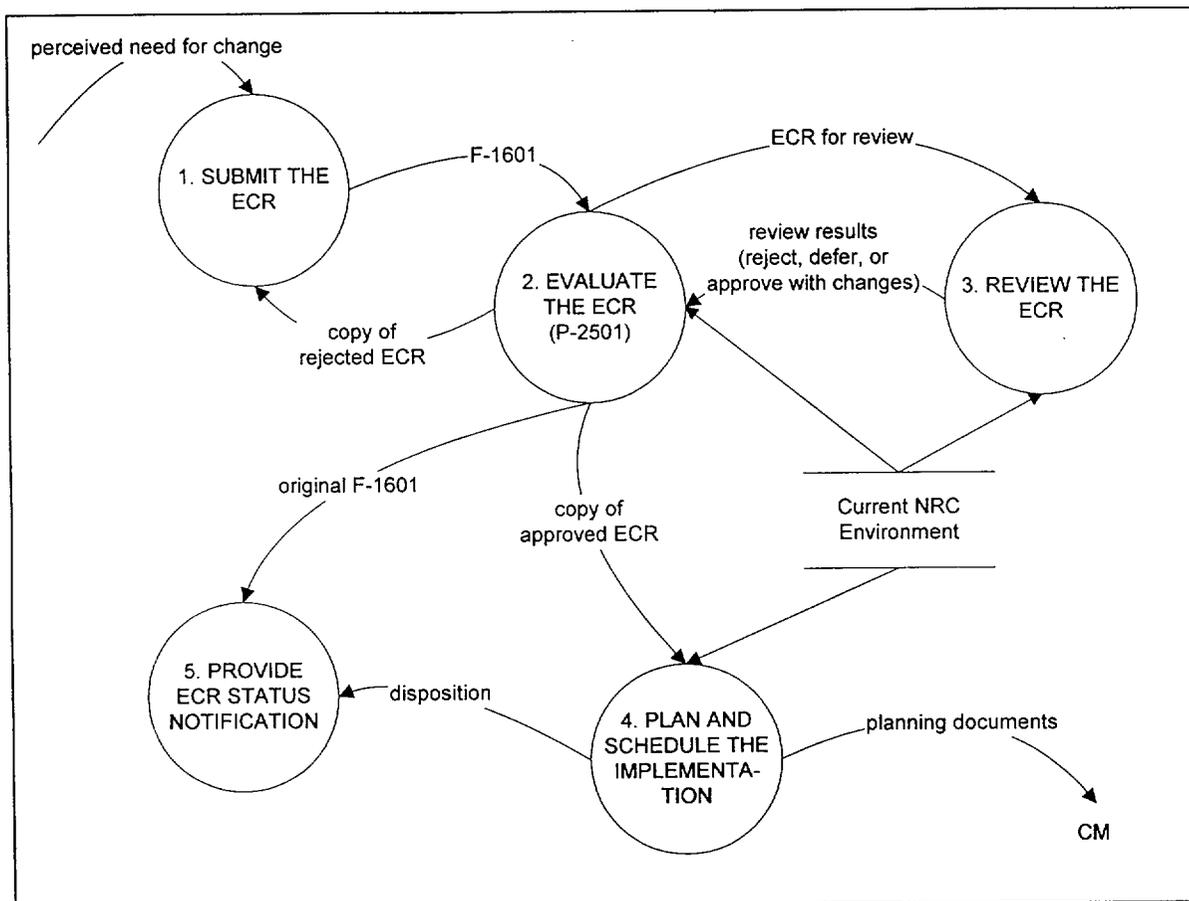


Figure 1601-1. Environment Change Data Flow Diagram

4.3 Steps

This section provides details of the steps shown in the data flow diagram (Figure 1601-1) and the data items that flow among the steps. The Step-Role table included in Section 4.6 clarifies which roles are responsible for performing which steps.

Perform the following steps:

1. Submit the Environment Change Request

Any NRC personnel and any personnel from NRC contractor organizations may submit an ECR. ECRs propose additions, deletions, or modifications to NRC's current environment².

To request a change, use SDLCM Methodology Form F-1601, Environment Change Request Form. Complete all blocks under "Originator Information" and "Change Information." Attach additional pages as needed to provide the required details, and use the form as a cover sheet to submit the request.

² See first footnote.

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

ECR Form Instructions

Originator Information

- ♦ Complete fields for Originator's Name, Organization, Location, Telephone Number, and Date Submitted.
- ♦ Provide the printed name of the Originator's Supervisor. Obtain the signature and date after completing the Change Information portion.

Change Information

- ♦ **Responsible NRC Organization.** Specify the NRC organization responsible for the environmental element to be changed.
- ♦ **Scope.** Check the applicable box.
- ♦ **Priority.** Check the applicable box. For a time-critical change, specify a deadline. For time-critical and urgent changes, provide a justification and state the effect of a delay in Part A, Items 6 and 7 (see below).
- ♦ **Brief name.** Provide a brief identification of the new hardware or software technology to facilitate references to your ECR.
- ♦ **Details.** Provide information that addresses each of the items in Parts A, B, and C, as applicable.

Part A. Enter the following information directly on the form or provide an attachment labeled "Part A." If an item does not apply, justify why not and specify "N/A."

1. Vendor Name
2. Complete name of new or expanded technology, including version, release, and patch identifiers, if applicable
3. Number of copies that will be needed
4. Number of desktops that will be affected by the presence of either the vendor product or the output generated by the vendor product (for example, run-time modules)
5. Source of funding to satisfy Items 3 and 4
6. Justification for Time-Critical or Urgent priority
7. Consequences of rejecting this request from the requestor's perspective (for example, a failure to meet an agreed-upon delivery date for a system as promised to the Commission)
8. Compatibility with the NRC's Technical Reference Model (Preferred or Target)
9. Required operating environment (hardware, operating system, or other products)
10. Intended functionality that this product, upgrade, or patch will offer
11. Summary of distinguishing features of the product, upgrade, or patch
12. Technological benefit to the NRC
13. Applicability of the product for other users, systems, platforms, etc. (for example, can others benefit from the change?)
14. Availability of a competing (or comparable) technology product already in the NRC environment (for example, for a new product request, is there a similar product already installed?)

Part B. Provide an attachment to the form labeled "Part B."

Using the criteria listed below, provide a comparative evaluation of the requested new or upgraded technology with at least two competing products. (If the answer to Part A, Item 14 is "yes," one of these must be the currently available product.)

For each of the criteria, rate each product numerically from 1 to 4 as follows: (1) Does not satisfy requirements, (2) Partially satisfies requirements, (3) Satisfies requirements, and (4) Exceeds requirements. Indicate not applicable (N/A) where appropriate. The first criterion (specifically required functionality) shall be weighted higher than the other criteria. Use a table or narrative as appropriate for your ECR. Provide any explanatory information needed to support your

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

evaluation. Conclude the comparison with a cost-benefit analysis that supports the Environment Change Request.

- a. Specifically required functionality
- b. Documentation support
- c. Y2K compliance
- d. Ease of installation, setup, and use
- e. On-line help
- f. Vendor training (specify costs if separate from purchase price)
- g. Vendor stability
- h. Product Stability
- i. Licensing requirements and issues (specify costs and whether site licensing is available)
- j. Upgrade to earlier version already in the environment

Part C. Optionally, provide an attachment to the form labeled "Part C" to present any other information in support of your Environment Change Request.

Submit the completed ECR form to the originator's supervisor for approval. **The supervisor submits the form to the CISSCO Configuration Management organization for processing** as defined in SDLCM Methodology Procedure P-2501, Configuration Control Board. CM processing includes reviewing the package for completeness, assigning an ECR number if complete, packaging the ECR along with other ECRs, and submission to the CCB. Review for completeness includes confirming the presence of all applicable information in Part A and a comparison of at least three products in Part B.

2. Evaluate the Environment Change Request

The NRC Environment CCB reviews the ECR (see Procedure P-2501).

In accordance with Procedure P-2501, the members review the ECR (or a package of ECRs) prior to the actual CCB meeting. Each CCB member's review includes, at a minimum, assessment of any effect on the member's area of responsibility. (For example, is there any effect on other environmental elements or any need for other upgrades to support the current change request?)

The CCB shall forward the ECR to the Change Review Committee to review its potential effect on the current environment³ (Step 3). This technical review will normally be completed prior to the scheduled CCB meeting so that the CCB members will be prepared to vote on the disposition of the ECR during the meeting.

If the CCB rejects the ECR, the form is annotated with the justification for the rejection, and the CM organization provides a copy of the ECR form to the originator.

If the CCB approves the ECR, CM forwards a copy to the Change Implementation Committee (Step 4).

The CCB may also decide to defer action until a future CCB meeting date, possibly to permit additional review by the Change Review Committee (Step 3).

³ See first footnote.

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

ECR Form Instructions

CCB Action

- Select one box to indicate the disposition of the ECR. Justify a rejected ECR in the Comments field. Specify a date for a deferred ECR.
- Provide the printed name and signature of the CCB Chairman. Indicate the date the ECR is signed.
- Comments. If applicable, provide comments from the CCB as feedback to the originator or for the record; attach additional pages if necessary.

3. Review the Environment Change Request

The Change Review Committee reviews the request for its potential effect on the current environment⁴. The committee members may request additional information from the originator. The committee documents its recommendations (including any possible implementation alternatives) and returns the ECR to the CCB for further evaluation (Step 2).

4. Plan and Schedule the Implementation

The Change Implementation Committee develops a plan, including a schedule, for implementing approved ECRs. If necessary, the committee members consult with a person or group possessing the necessary expertise or experience (possibly the originator). A copy of the reviewed and approved plan is placed under CM control.

5. Provide Environment Change Request Status Notification

The Chairman of the Environment CCB sends an e-mail notification to all personnel within the Office of the Chief Information Officer and to the members of the Information Technology Business Council announcing the nature of the change and the schedule for implementation.

The CM organization notifies the requester of the final disposition of the ECR.

The CM organization maintains the status of all ECRs; ECR status is available for review by any personnel throughout the environment change process.

4.4 Exit Criteria

The outputs of this procedure are:

- A completed Environment Change Request Form maintained by CM
- All information required to update the environment if the request was approved
- Information necessary to update the applicable NRC inventory

The results of the procedure are:

- The ECR is approved; a plan and schedule have been prepared and placed under CM control.
- Alternatively, the originator understands why the change request was rejected

⁴ See first footnote.

Subject Environment Change	Type	Procedure
	Identifier	P-1601
	Effective Date	December 1999
	Revision No.	

4.5 Verification

Quality Assurance personnel verify that this procedure is followed and that all outputs are filed.

4.6 Roles

Table 1601-1 depicts the roles responsible for each step in the Environment Change procedure.

Table 1601-1. Environment Change Step-Role Table

Steps	Roles:	Change Request Originator	NRC Environment CCB	Change Review Committee	Change Implementation Committee	CM
Submit the ECR		P				R
Evaluate the ECR			P			S
Review the ECR		S	A	P		S
Plan and Schedule the Implementation		S	A	R	P	S
Provide ECR Status Notification			P			P

Legend: P=Performs, R=Reviews, A=Approves, S=Supports

Note: The NRC CIO (or his or her designee) appoints the members of the NRC Environment CCB. The chairman of the Environment CCB appoints the members of the Change Review Committee and the Change Implementation Committee.



OPERATIONS CONFIGURATION CONTROL BOARD (OPS CCB) CHARTER

Purpose:

The purpose of this document is to delineate the responsibilities and processes for changes to the operational infrastructure at the U.S. Nuclear Regulatory Commission (NRC).

Reason:

The integrity of the operational infrastructure is the responsibility of the Office of the Chief Information Officer, Information Technology Infrastructure Division. All changes to the operational infrastructure (from desktop to the LAN/WAN, hardware and software) must be controlled in order to maintain the integrity of the infrastructure and to provide the U.S. NRC with a stable infrastructure. The OPS CCB will ensure that all changes to the operational infrastructure are coordinated, tested and documented prior to their implementation.

Applicability:

All proposed changes to be made to the operational infrastructure shall be submitted to and approved by the OPS CCB. This process complements the SDLCM and IDPM development models. The OPS CCB is the process by which products developed through the SDLCM and IDPM, as well as commercial products are integrated into the NRC's operational environment.

Configuration Control Board process:

- The change initiator shall prepare a Technical Change Request (TCR). The initiator shall ensure that the change has been coordinated with all affected parties, tested, and communication prepared announcing the change. The TCR form is available on the IT CSB homepage.
- The TCR will be submitted to the Configuration Manager for inclusion on the OPS CCB agenda.
- The OPS CCB will review and approve the change, and oversee the management of the release deployment when applicable.
- Minutes of the OPS CCB will be prepared and distributed at the following meeting.
- A matrix of approved changes will be published and maintained on the IT CSB intranet homepage.
- Emergency TCR's should be the exception rather than the rule. The same information is required of emergency TCR's. Submission of emergency TCR's is made to the Chief, IT Customer Services Branch for review and approval.

Meetings:

The OPS CCB will meet every Wednesday. An agenda will be distributed before the meeting. Representation at the OPS CCB will include at a minimum ITID/IDIB, ITID/CSB, ADD, and the Regions. The Chief, IT Customer Services Branch will chair the meeting.

APPROVED:

James B. Schaeffer
Director, ITID

Arnold (Moe) Levin
Director, ADD

OPERATIONS CCB CHANGE CHECKLIST

- Has the contents of the change been identified?
- Has the impact of the change been identified? (i.e., agencywide, floor xx, internet services, etc.)
- Has the change been coordinated with all affected parties?
 - ADAMS
 - STARFIRE
 - ADD
 - Operations
 - Customer Support Center
 - Regions
 - Customers

Communication:

- Has the network bulletin been prepared?
 - Does the bulletin go agencywide or HQ only
- IT Coordinators/regions notified/coordinated with?

Test Results:

- Has the change been tested? (functionality, test lab)

Documentation:

- Users guide prepared?
- Operational Support Guide prepared?

Deployment Strategy:

- Phased deployment?
- Public workstations accounted for?
- IT Coordinator multiple logins accounted for in regions?

REMOTE ACCESS

Background

The U.S. Nuclear Regulatory Commission (NRC) has a mission support requirement for nuclear inspectors and others to be able to access the NRC wide area network (WAN) remotely. This remote access support has been provided for almost six months utilizing CITRIX MetaFrame technology. The Remote Access System (RAS) calls for deployment at the following sites: NRC Headquarters (HQ), Regional Offices (RO), all Resident Inspector System Expansion (RISE) sites and NRC employees who require access from home or while traveling. Ongoing support of remote end-users remains the responsibility of the NRC support staff.

1.1 Remote Access (RA)

RA refers to an ability to connect to the NRC WAN from a location which does not have a permanent connection. The NRC WAN includes NRC HQ, the four ROs, the Technical Training Center (TTC), and the RISE sites. Users working at these locations are local users, and are not using remote access. The term remote always refers to the computer that is not physically connected to the NRC WAN.

The primary group of RA end-users is NRC staff working from home or on travel. The Remote Access System (RAS) also provides backup connectivity for RISE sites. All an end-user needs is an NRC RAS account and password, the correct software installed on their computer, and access to a modem and phone line. When a user dials in to an RA server (host) a connection is established. Once an RA user has successfully logged in, he/she is able to access software and systems normally used at work.

2.0 Scope

The Remote Access System (RAS) has six components and defining the scope of what should be supported in an RA environment is challenging. This section will clarify what will be considered part of RA support.

2.1 Scope of the Remote Access System

Figure 1 illustrates the Remote Access System (RAS) components and how these elements are connected. The six components are listed below:

1. Remote Computer or Laptop (Client)
2. Telecommunications
3. NORTEL 5399 Remote Access Concentrator
4. ERPCD Authentication Server
5. CITRIX MetaFrame Server
6. NRC Wide Area Network (WAN)

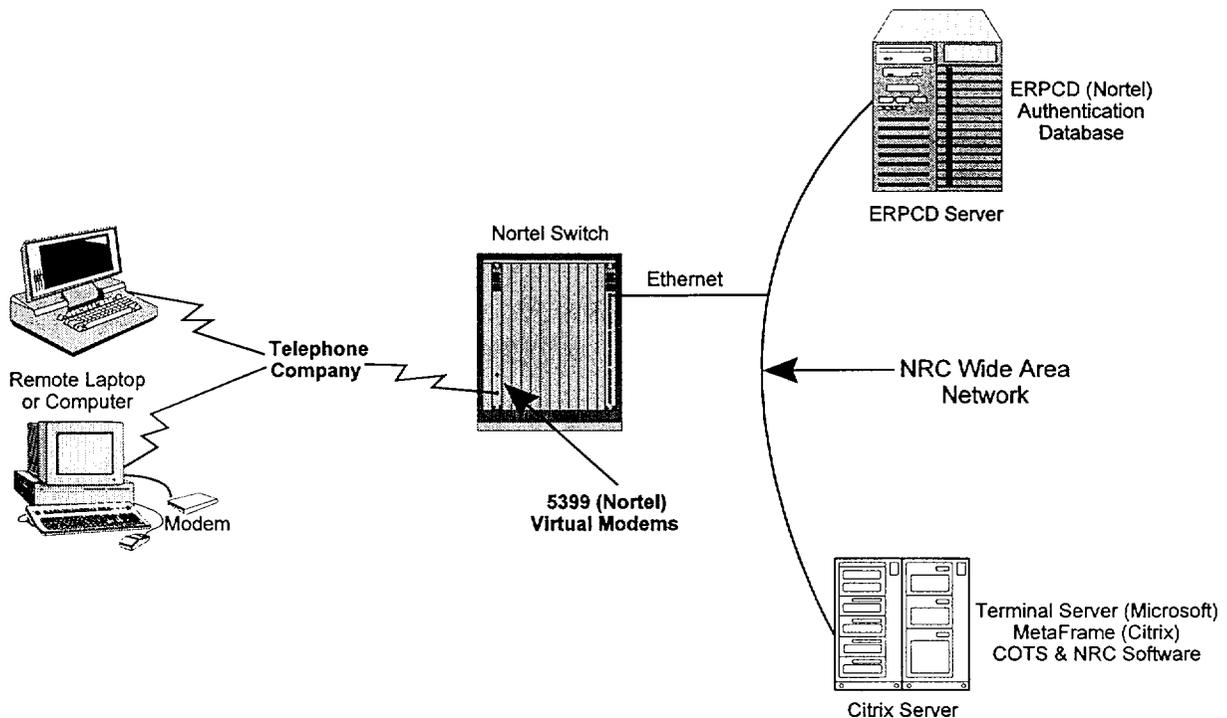


Figure 1: Remote Access System Components

2.1.1 Remote Computer or Laptop

The first component of the RA system is the remote computer or laptop (client). An end-user initiates the connection sequence by dialing in from a remote computer via a telephone line using a modem. The minimum hardware and software requirements are listed below:

- 486 or Pentium class PC, keyboard and mouse (with a clock speed of at least 33 Megahertz)
- SVGA monitor with 1 MB of video memory
- 10 MB free hard disk space
- 32 MB or more RAM
- 28.8 Kbps or higher modem (internal or external) (See the CITRIX Modem Compatibility List - Attachment A)
- Windows 95/98 or NT operating system installed
- RAS v3.0 installed

2.1.2 Telecommunications

The second component of the RA system is the telephone circuit (Figure 2). An end-user initiates the connection sequence by dialing in from a remote computer via a telephone line using a modem. The signal travels through the telephone system and connects to the NRC via a PRI ISDN line into the NORTEL 5399. The PRI ISDN line supports up to twenty-three 64KB access lines from the telephone company. The hardware requirements and software configurations depend on the local telephone provider (e.g. Bell Atlantic).

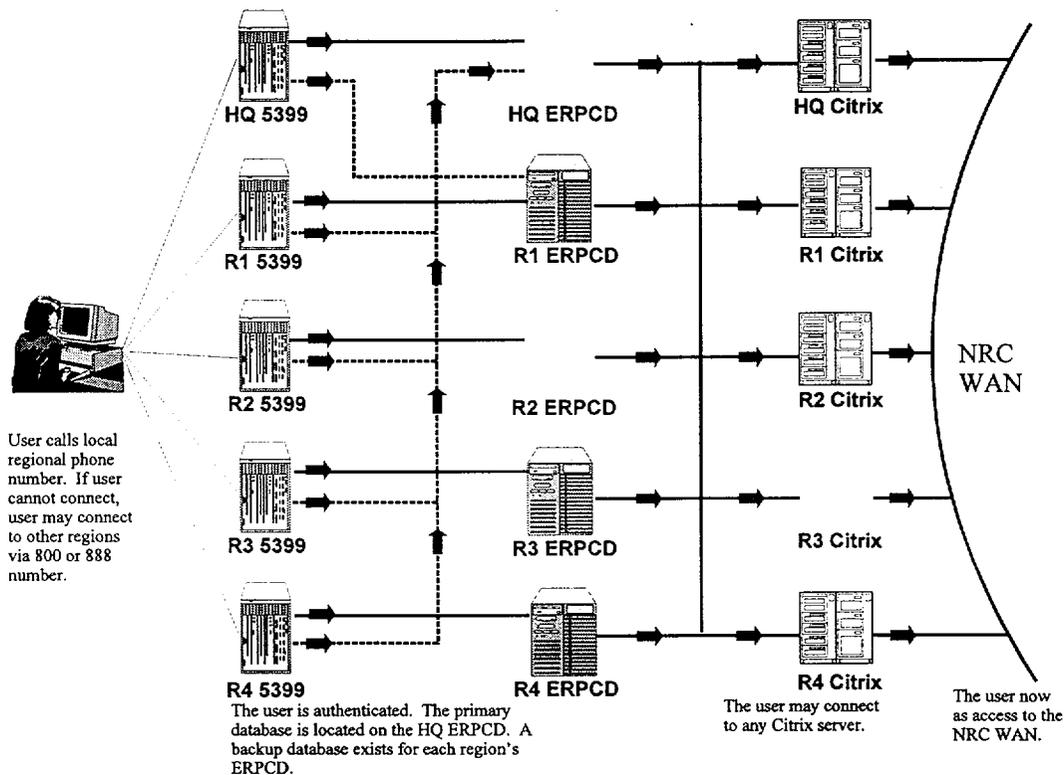


Figure 2: Dial-in Pathways

2.1.3 NORTEL 5399 Remote Access Concentrator

The third component of the RA system is the NORTEL 5399 Remote Access Concentrator (RAC). The NORTEL 5399 provides a bank of virtual modems which allow a remote connection. This digital modem technology enables dial in pooling which provides RA end-users with maximum performance. The 5399 board supports 24 to 48 dial in lines. For industry standards and specifications see <http://www.baynetworks.com/products/datasheets/>.

2.1.4 ERPCD Authentication Server

The fourth component of the RA system is the ERPCD Authentication server. This security service software runs on a Windows NT Backup Domain Controller (BDC). The NORTEL 5399 passes the user ID and password to the ERPCD Authentication server. This server functions as the first level of security. It verifies the end-user by checking logins against the local ERPCD database. The NOC is responsible for creating user accounts in the database. Accuracy is critical, because one character out of place will lock-up the database.

2.1.5 CITRIX MetaFrame Server

The fifth component of the RA system is the CITRIX MetaFrame Server. Once an end-user has been verified by the ERPCD as being a bonafide user, the user is provided access to the NRC WAN, and the user session is directed to a CITRIX MetaFrame Server. The user must login to the network (second security check). The NRC's CITRIX servers are licensed to support up to 25 concurrent RA sessions. When an end-user successfully logs in to the Windows NT Domain and Novell NDS tree, through the server, they are able to access all of the NRC NGN resources.

2.1.6 NRC Wide Area Network

The sixth and final component of the RA system is the NRC Wide Area Network (WAN). The WAN software contains standard applications (e.g., Corel Suite, GroupWise, etc.), Agency applications (e.g., ADAMS, RPS, etc.) and end-user data. The RAS connection sequence is complete when the end-user has access to NRC NGN applications, and Agency and personal data.

DMZ/ FIREWALL

Zone 1: National Institute of Health (NIH) DMZ

Functions:

The NIH DMZ is the primary entry point to the NRC network from the Internet. Physically, it is between the National Institute of Health, the NRC Internet Service Provider (ISP), and the NRC network. This zone is created to audit the inbound traffic from the Internet to the NRC network.

Services:

1. Internet connectivity from the NRC network.
2. Internet connectivity to the NRC from the Internet.
3. PayPers.
4. INPO

Components:

1. IDS1 engine.
2. FWR1 router
3. NIHE1 hub.

Zone 2: Internet DMZ

Functions:

The DMZ zone is designed to support the NRC primary Internet services such as Email, outbound/inbound web access, FTP & Tenet proxy, and Virtual Private Network (VPN). Physically, it's between FWR1 and NGN_WNR1). The DMZ zone includes subnet 176 and subnet 174.

Services:

1. SMTP mail.
2. External DNS.
3. DNS forwarder for internal DNS servers (DNS1, DNS2 & DNS3).
4. DNS forwarder for the internal proxy server (IRM70)
5. Proxy service for the internal proxy server via Socks.
6. Telnet & FTP proxy.
7. Internet News
8. Trusted user jump-off point.
9. Dial-up access via the NetBlazer.
10. NRC main external web site.
11. Anonymous FTP service.
12. DMZ bandwidth measurement.
13. Outbound intrusion detection engine.
14. Virtual Private Network.

Components:

1. IGATE.
2. IGATE2.
3. AGATE
4. WWW
5. IGATE4
6. IGATE3
7. IDS2

8. NGN_WNR1 router
9. DMZE3 hub
10. DMZE1 hub
11. FWE1 hub

Zone 3: Public Access Area 1 (PAA1) DMZ (Not yet fully deployed)

Functions:

The PAA1 zone is one of two DMZ zones that are controlled by a Cisco PIX firewall. Both PAA zones are designed to add additional monitor and countermeasure capabilities to the NRC firewall to counter additional inherited risks of those services that resides in the PAA zones. PAA1 zone controls and audits access to three of the agency public services: ADAMS, Electronics Information Exchange (EIE) and Public Document Room (PDR). Each of those service has its own network segment and custom access control list (on the PIX firewall). The PAA1 zone is connected to the NRC firewall through FWR1.

Services:

1. ADAMS
2. EIE
3. PDR

Hosts:

1. PAA1 firewall (not yet deployed)
2. PBNTAD01
3. PBNTAD02
4. PBNTAD03
5. PBNTAD04
6. EIE
7. PDHost (server)
8. PDR workstations (four)
9. HOSTE1 hub
10. DMZE4 hub
11. DMZE5 hub (not yet deployed)

Zone 4: Public Access Area 2 (PAA2) DMZ (Not yet fully deployed)

Functions:

The PAA2 DMZ zone is one of the two Public Access Area DMZ zones that are controlled by a Cisco PIX firewall. The PAA2 zone is designed to share the load of the Internet DMZ zone by moving the NRC external web service and the Netblazer Dial-up access from the Internet DMZ to the PAA2 DMZ. The PAA2 zone has three available network segments that can be used to support future Internet applications.

Services:

1. NRC external web service.
2. Dial-up access via the NetBlazer.

Components:

1. PAA2 Firewall (not yet deployed)
2. WWW
3. AGATE
4. DMZE6 hub (not yet deployed)

Zone 5: The Foreign Networks (FN) DMZ

Functions:

The Foreign Networks (FN) DMZ is designed to audit and control access to the NRC contractor sites. Although each network in the FN DMZ is part of the NRC WAN, and meets the same security criteria for network and personnel as the rest of the NRC WAN, they are not physically located in the agency headquarter complex.

Services:

1. Connectivity to CNWRA in San Antonio
2. Connectivity to CNWRA branch at TwinBrook, Maryland.
3. Connectivity to INEEL in Idaho.
4. Connectivity to CSC at Shady Grove, Maryland.
5. Connectivity to AMS at Executive Blvd, Maryland.

Components:

1. FNR1 router
2. FNE1 hub
3. CSR1 router
4. NGN_CSR1 router
5. TBR1 router
6. SAR1 router
7. EBR1 router

NRC Data Backup Media Retention Requirements

This document identifies the functions and expectations for backing up the NRC data from Novell, NT and Unix

1.0 Requirements

Data created and maintained by the NRC is stored on Novell servers, Windows NT servers and Unix systems as well as locally on NRC standard Windows NT workstations. This data must be safeguarded and be recoverable from corruption or deletion. Currently, a system of 8mm tape backup units function as the prime data backup for the Novell and non-ADAMS NT servers. The backups are run every evening Monday through Friday and include all data on all volumes (drives) on each Windows NT and NOVELL server. Unix systems are backed up by individually attached tape systems where incremental backups are performed each evening with a monthly full backup. Currently local workstations are not backed up via the network with this tape system.

The current requirements for data backup are as follows:

- Any system be fully recoverable from the last business day. This means that any Novell, NT, or Unix server can be restored to previous operating condition by only installing the parent NOS, and tape access software. All other data, system information, and account security information will be restored from backup without lengthy customization.
- That all backups include system security and user account information each and every time it is backed up including but not limited to all NT server registries and all Novell NDS information..
- That any file or segment of data be recoverable from the media in less than one hour.
- That back-ups run and be completed between 9pm and 6am weekdays.
- That the medium be removable and that the medium is routinely rotated off-site for disaster recovery. Backup media is rotated off-site each Monday from the previous Friday backup and returned the following Monday at which point the media is re-introduced into the data backup system.
- The data backup system should be capable of backing up NT workstations remotely over the existing infrastructure.
- Backup system must use conventional and tested technology and have accurate MTBF figures and extended warranty options.
- All backup media has to be readily available to OCIO staff and contractors in order to perform data restorations within 1 hour. Backup media must be retained for 10 business days. After 10 business days, the backup media is re-introduced into the backup cycle and re-used.

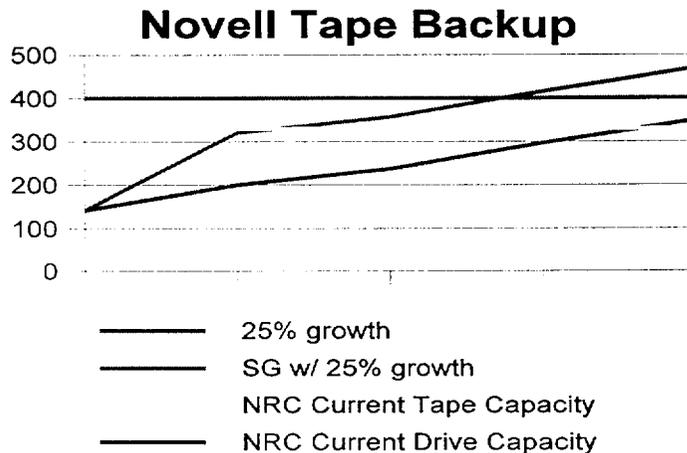
- OCIO staff and contractors must have the capability to monitor backup completion status to ensure the backup system is functioning properly.
- Periodic restorations are performed to validate backup system functionality.

	Current Data Backed Up	Current Total Disk Space	Anticipated Growth /Year
Novell (HQ)	200 GB	400 GB	25%
Novell (Reg)	145 GB		
NT	65 GB	230 GB	25%
Unix	500 GB	N/A	10%

2.0 Novell

Environment:

Currently, all Headquarters Novell data is being backed up to two 80 tape Mammoth tape systems. The Regional offices are using smaller tape systems which house 10 - 20 tapes. Each tape has an uncompressed storage capacity of 20 GB. A full uncompressed backup is performed nightly. Off site storage is performed on a weekly basis.



Statistics:

- Hard disk Capacity = 400GB
- Tape Backup Capacity = 330GB

- Current data backed up = 200GB
- Historical Annual Growth = 25%

Issues:

If the 25% current disk usage growth trend continues the Novell portion of the NRC backup system will not reach capacity in its current full nightly rotation until late 2003. It is anticipated that there will be a substantial change in drive usage and capacity due to the following factors:

- Shady Groves new server SGNWAS1 is currently on line with 90 GB of disk space capacity with 40 GB of disk space to be used in the near future.
- Starfire development server OOWNWAS2 is low on disk space and drives amounting to 20GB increased capacity have already been ordered and delivered.

Solution:

Tape drive capacity issues can be resolved with either increasing the tape drive capacity of the system by:

- Investing in additional hardware to increase current capacity
- Using the "StorageTek" tape silos, an existing system in the data center to perform data backups.
- Change backup schema from full nightly to incremental.

3.0 NT

Environment:

Currently, all Headquarters NT data is being backed up to one 80 tape Mammoths tape systems. Each tape has an uncompressed storage capacity of 20 GB. A full backup is performed nightly. Off site storage is performed on a weekly basis.

Statistics:

- Hard disk Capacity = 230GB
- Tape Backup Capacity = 160GB
- Current data backed up = 65GB
- Anticipated Annual Growth = 25%

4.0 Unix

Environment:

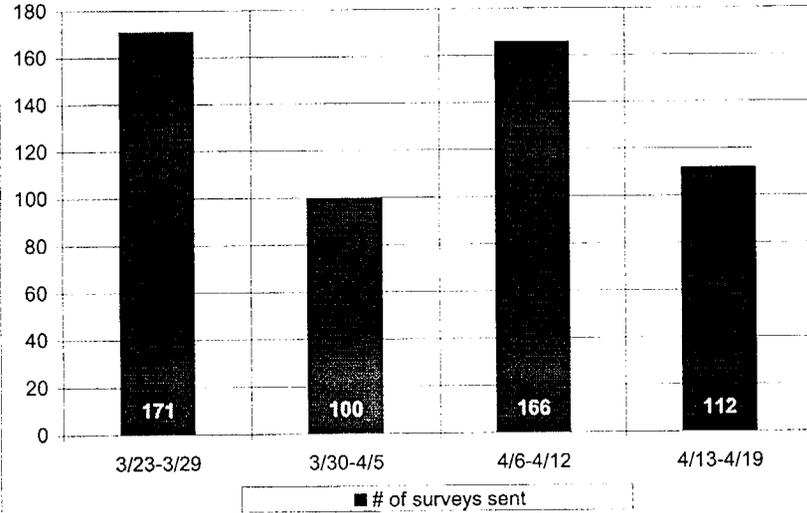
Currently, all Headquarters Unix systems are backed up by individually attached tape systems and are incremental with a monthly full backup.

Statistics:

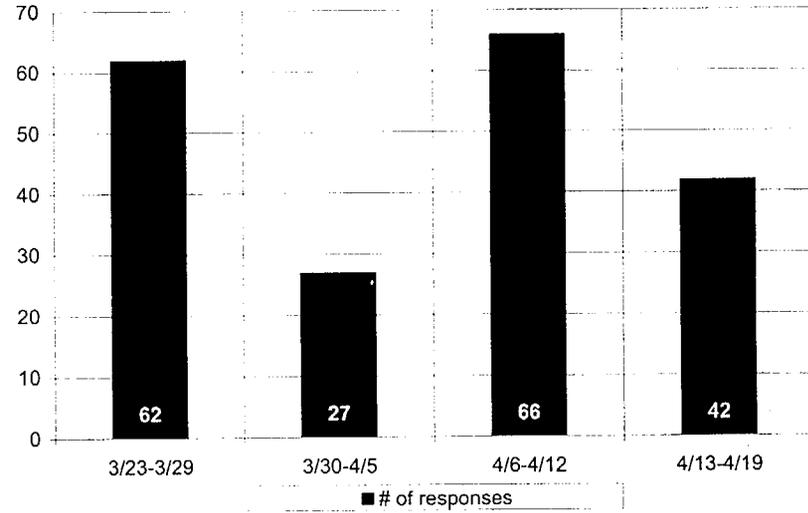
- Hard disk Capacity = ?GB
- Tape Backup Capacity = ?GB
- Current data backed up = 500GB
- Anticipated Annual Growth = 10%

CSC Survey Statistics (a/o 4/23/01)

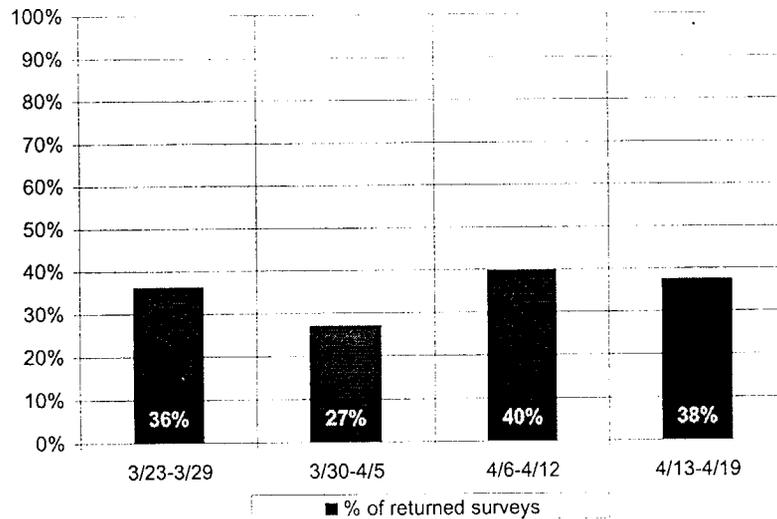
Surveys Sent



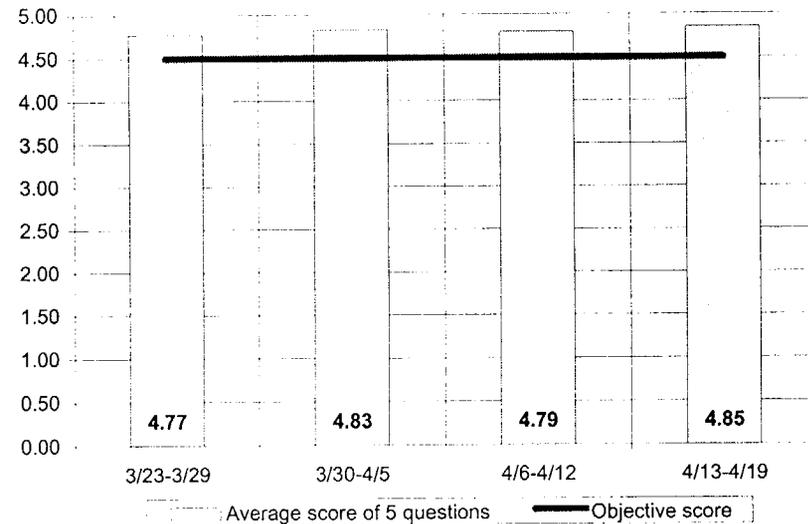
Number of Responses



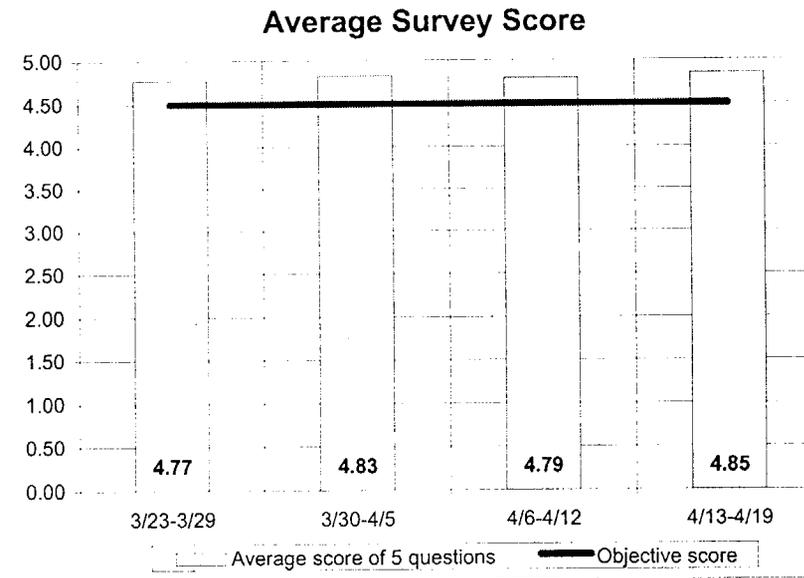
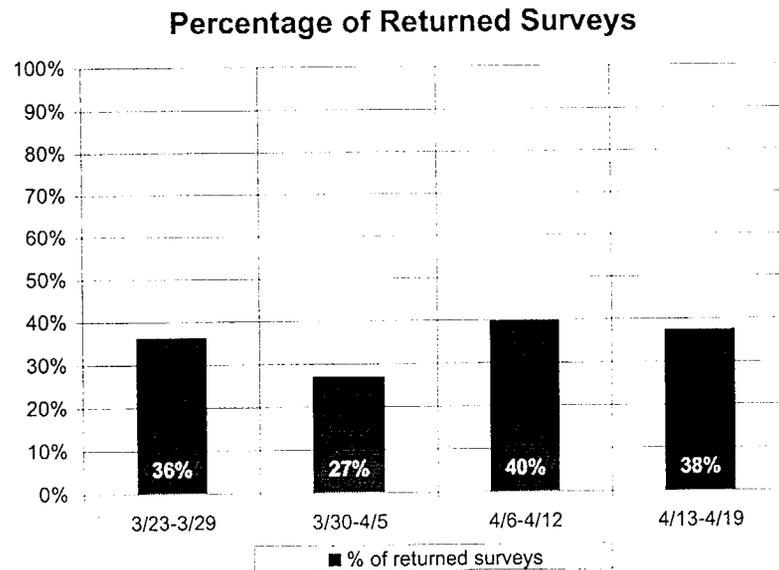
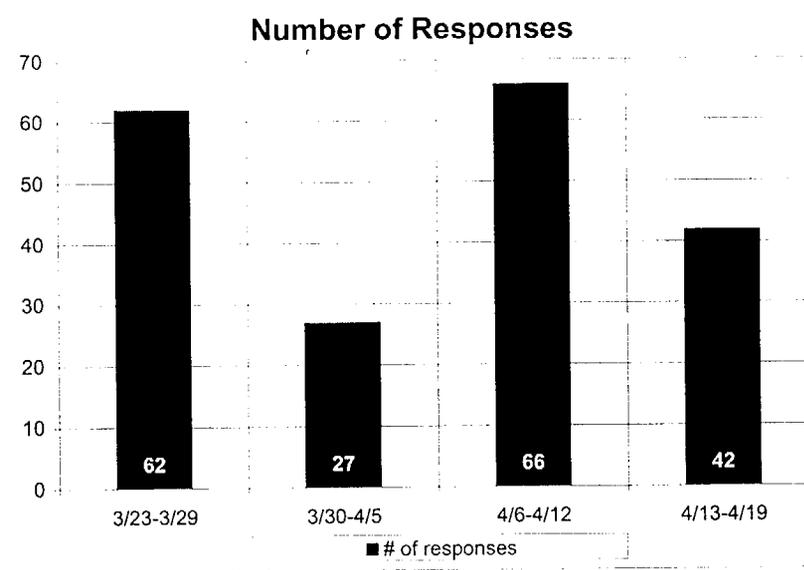
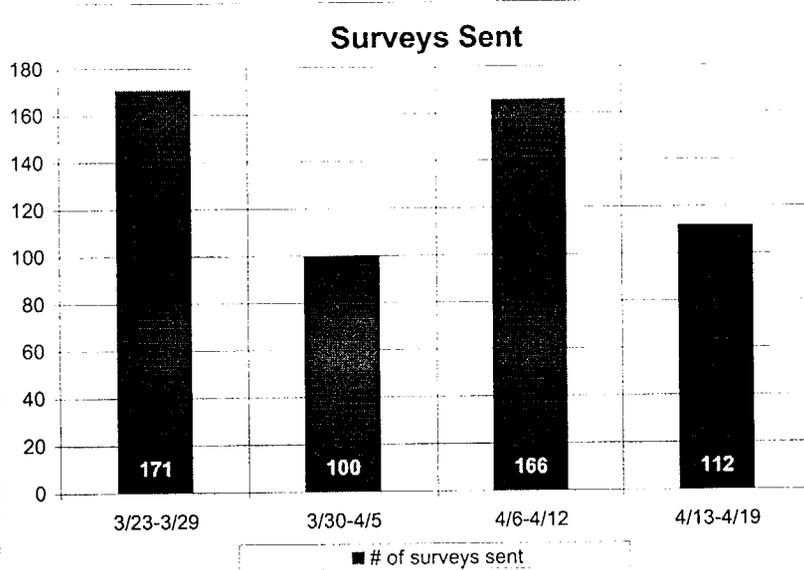
Percentage of Returned Surveys



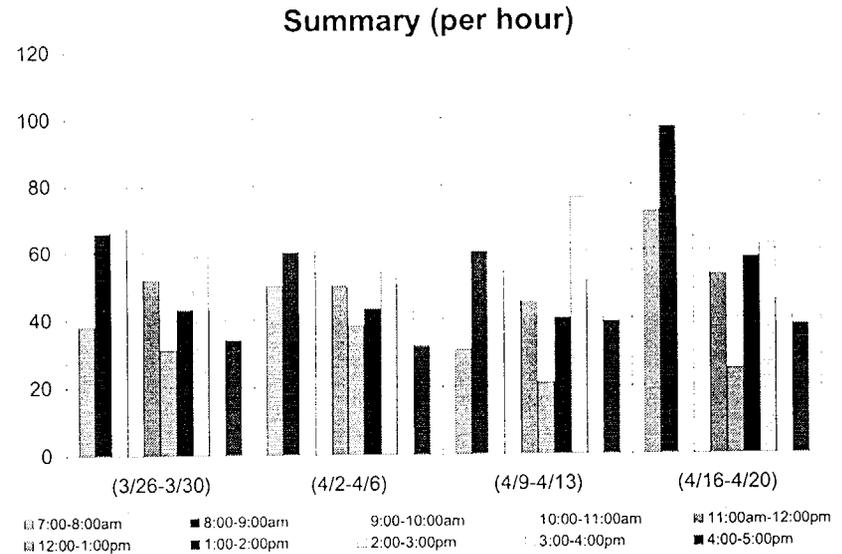
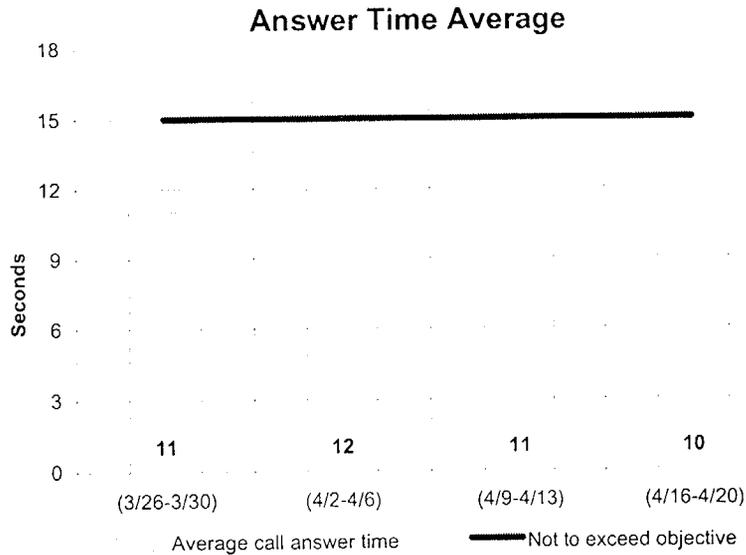
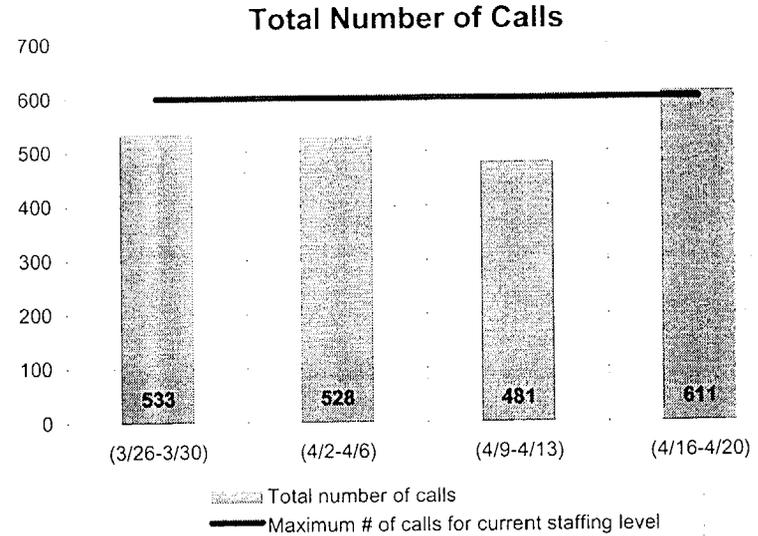
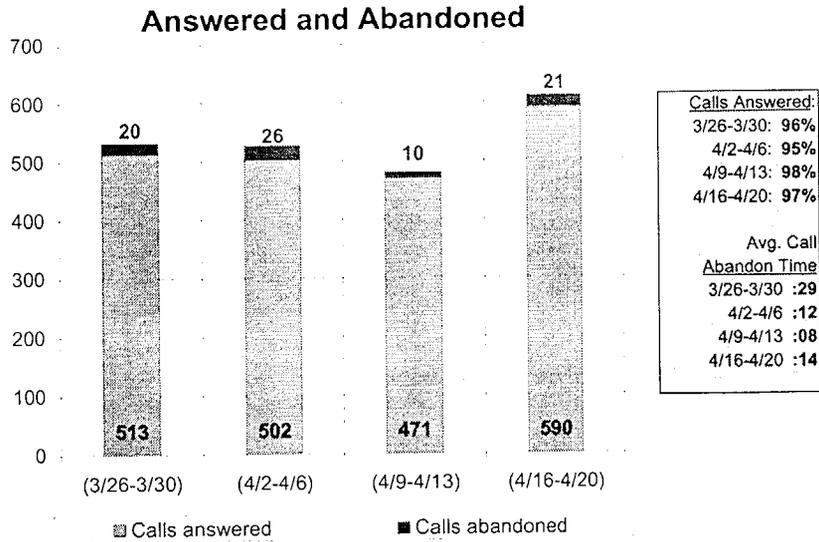
Average Survey Score



CSC Survey Statistics (a/o 4/23/01)

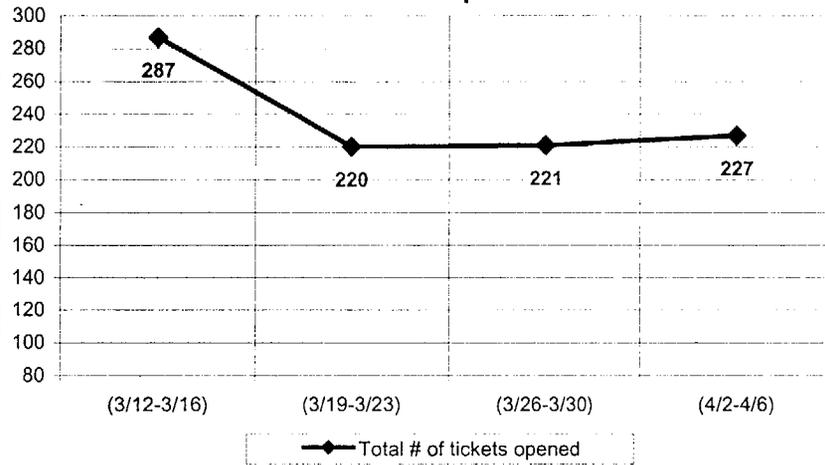


CSC Weekly Call Statistics (a/o 4/30/01)

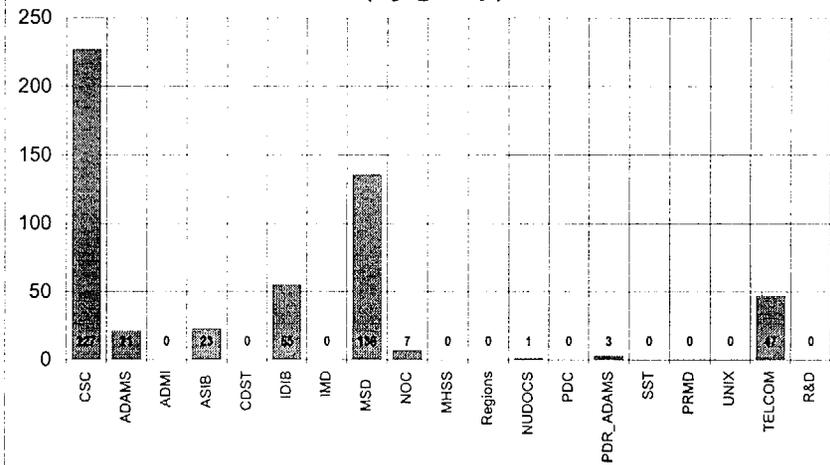


CSC Weekly Ticket Statistics (a/o 4/16/01)

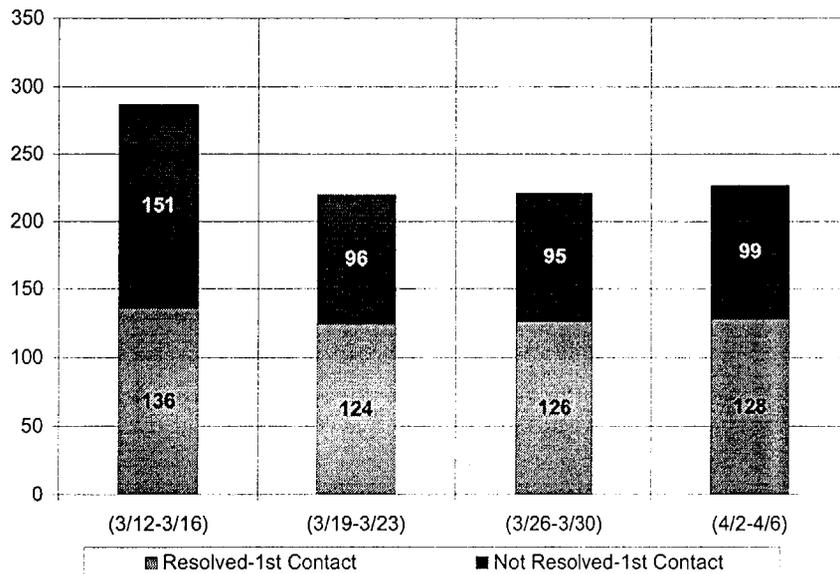
Tickets Opened



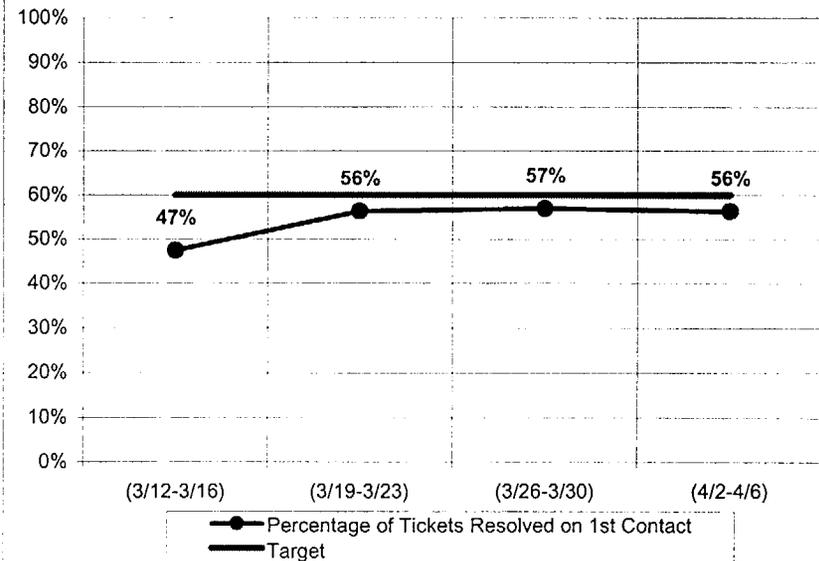
Distribution (by group) for 4/2-4/6



1st Level Resolution

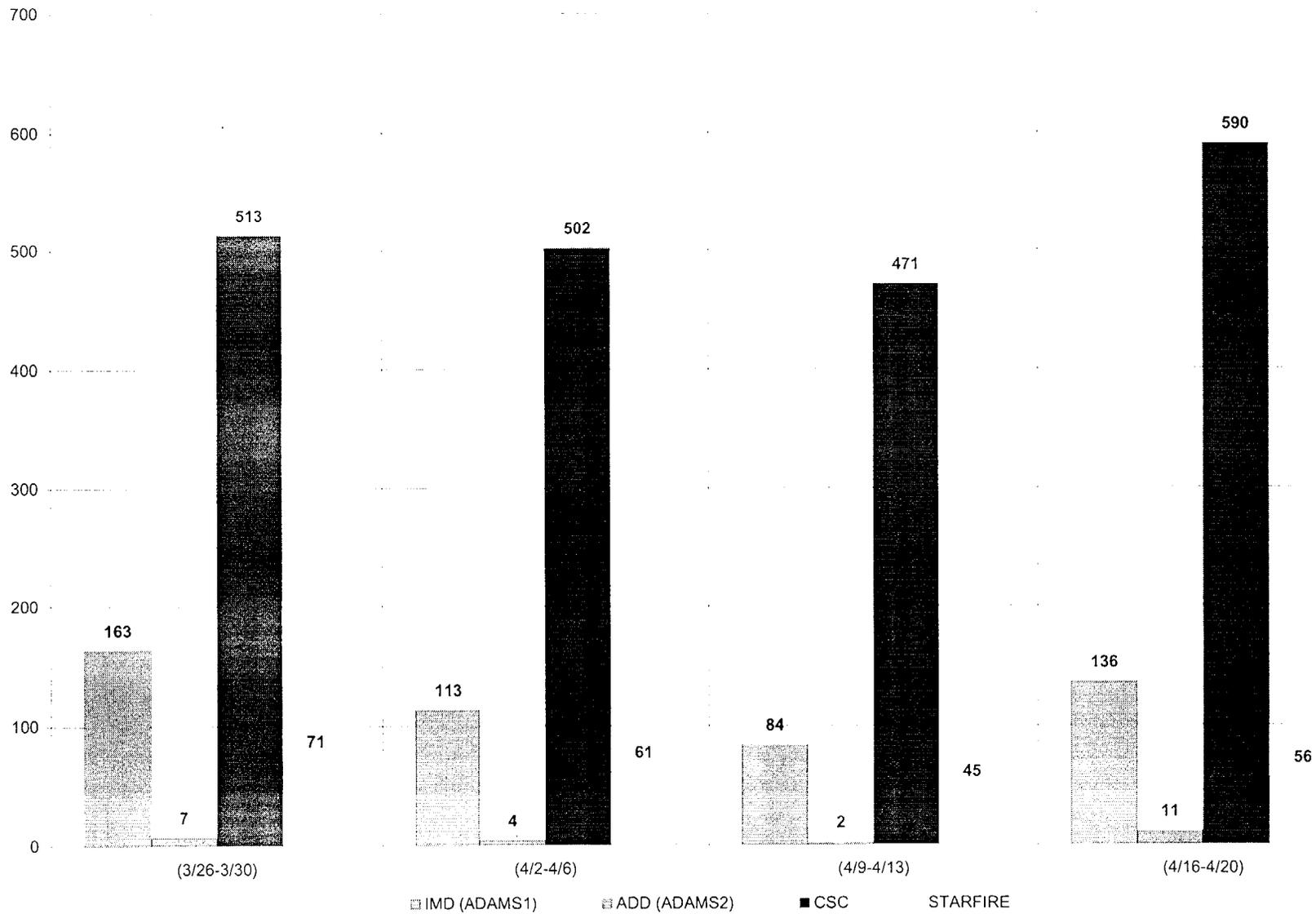


Percentage of Tickets Resolved on 1st Contact



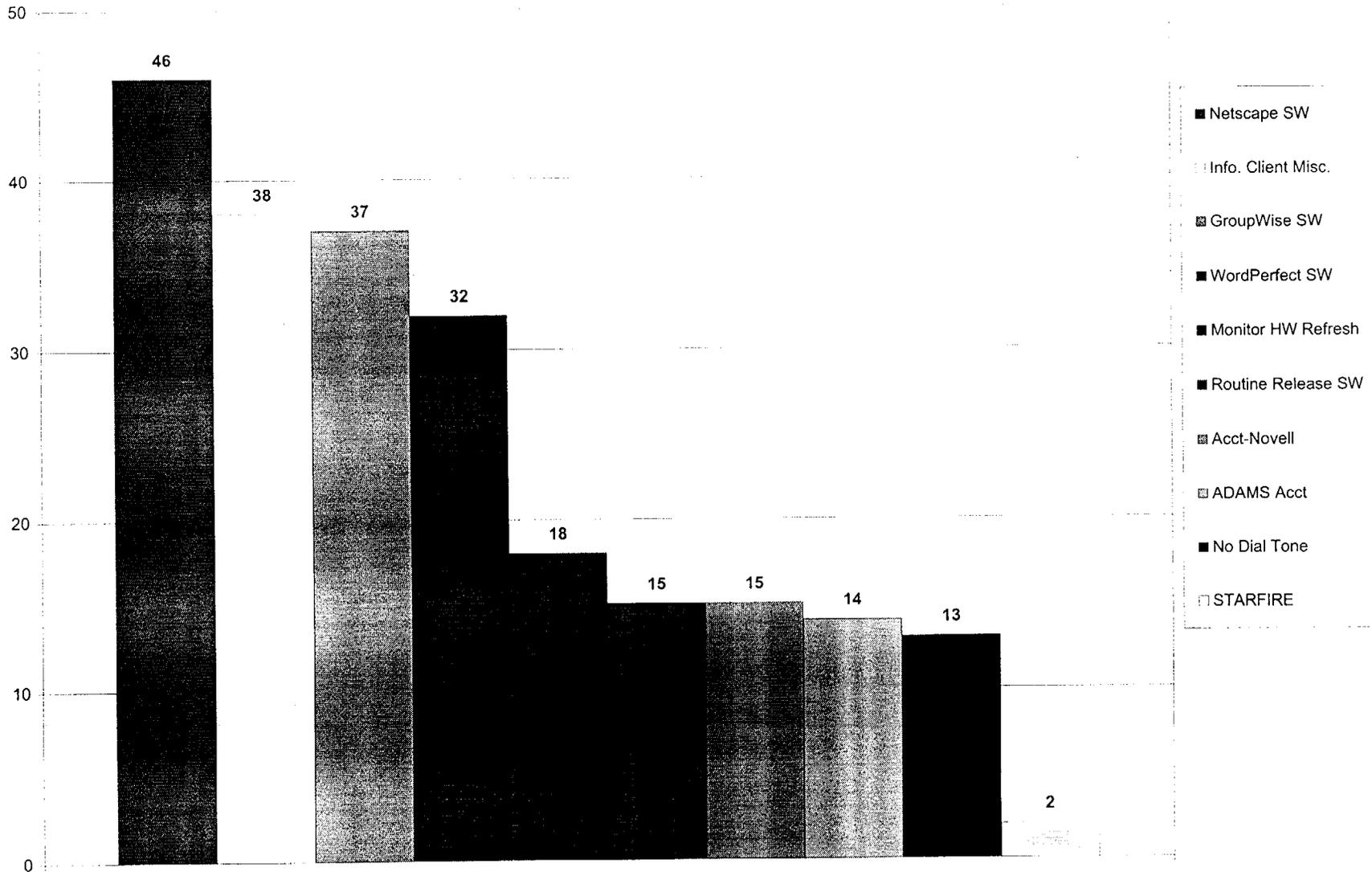
Lucent CMS Weekly Call Statistics (a/o 4/30/01)

Call Volume



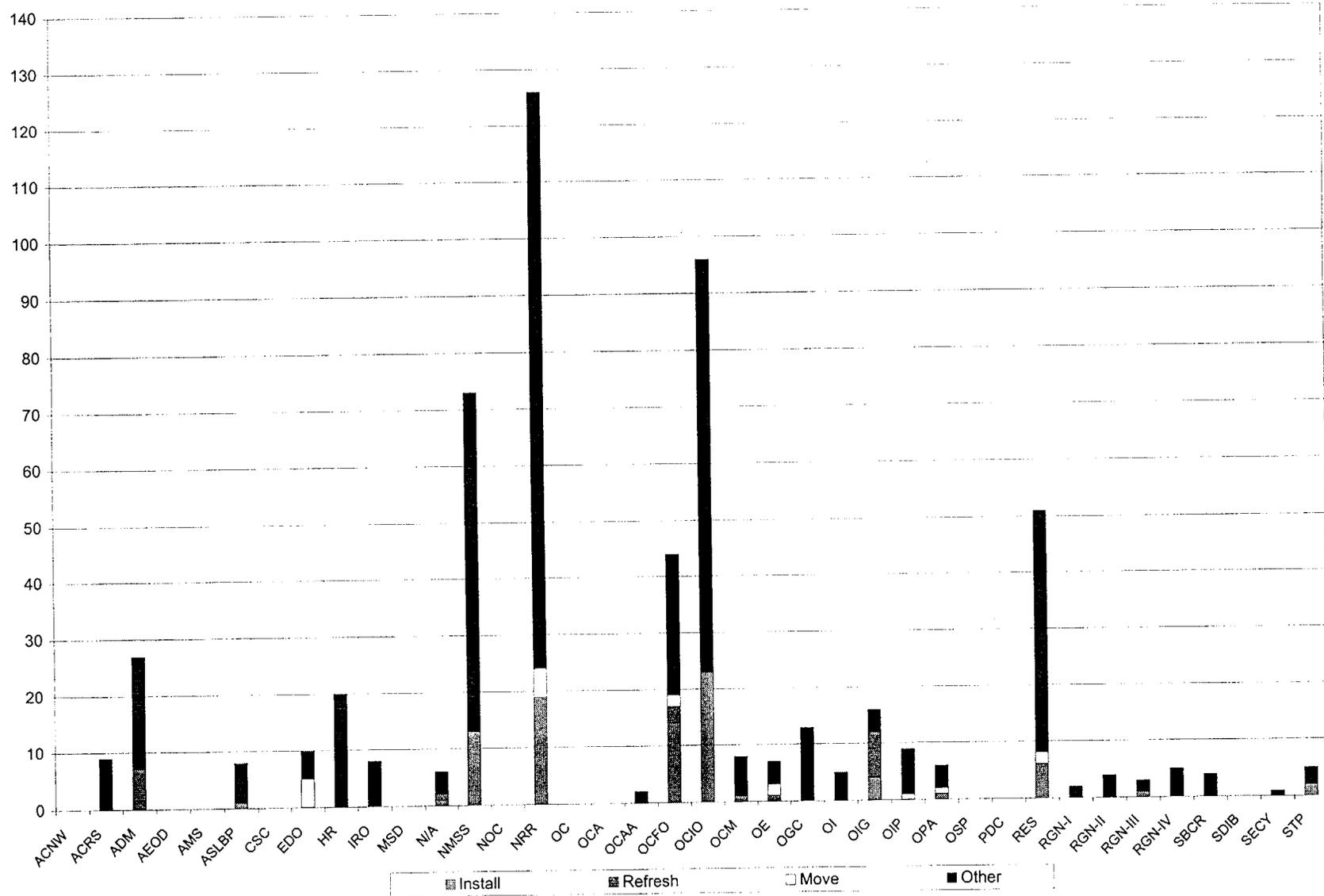
CSC Weekly Call Statistics (a/o 4/30/01)

Top Ten Ticket Category Breakdown (by type) 4/16-4/20

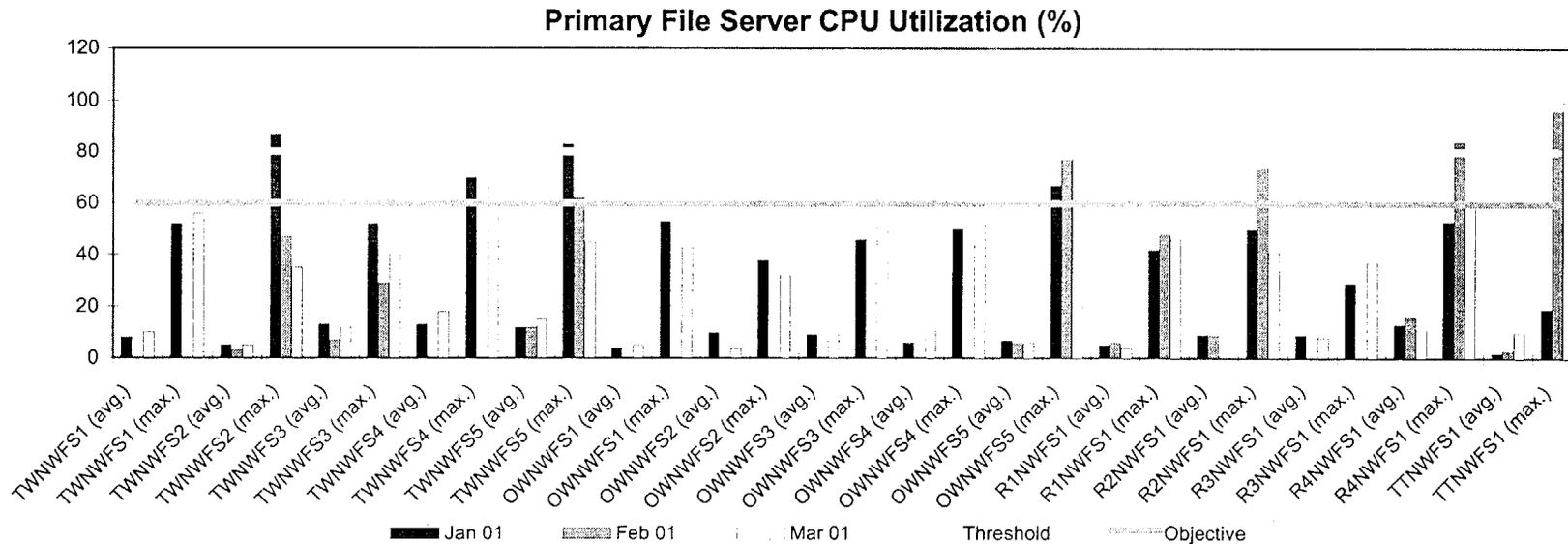
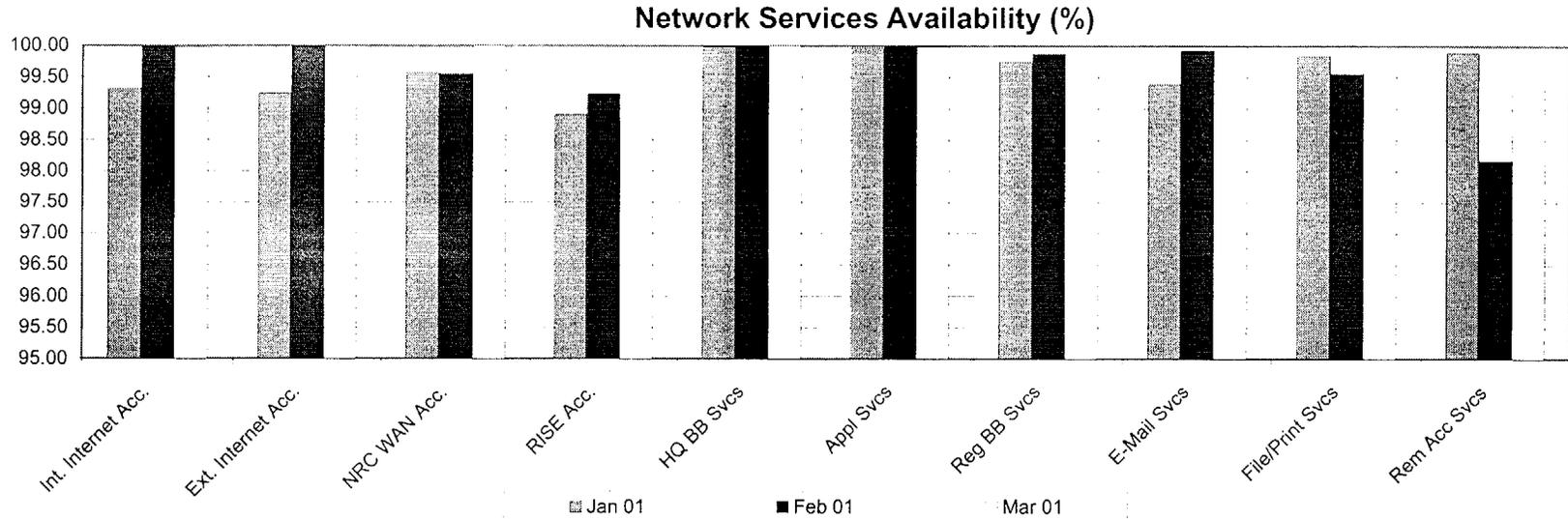


CSC Weekly Ticket Statistics (a/o 4/30/01)

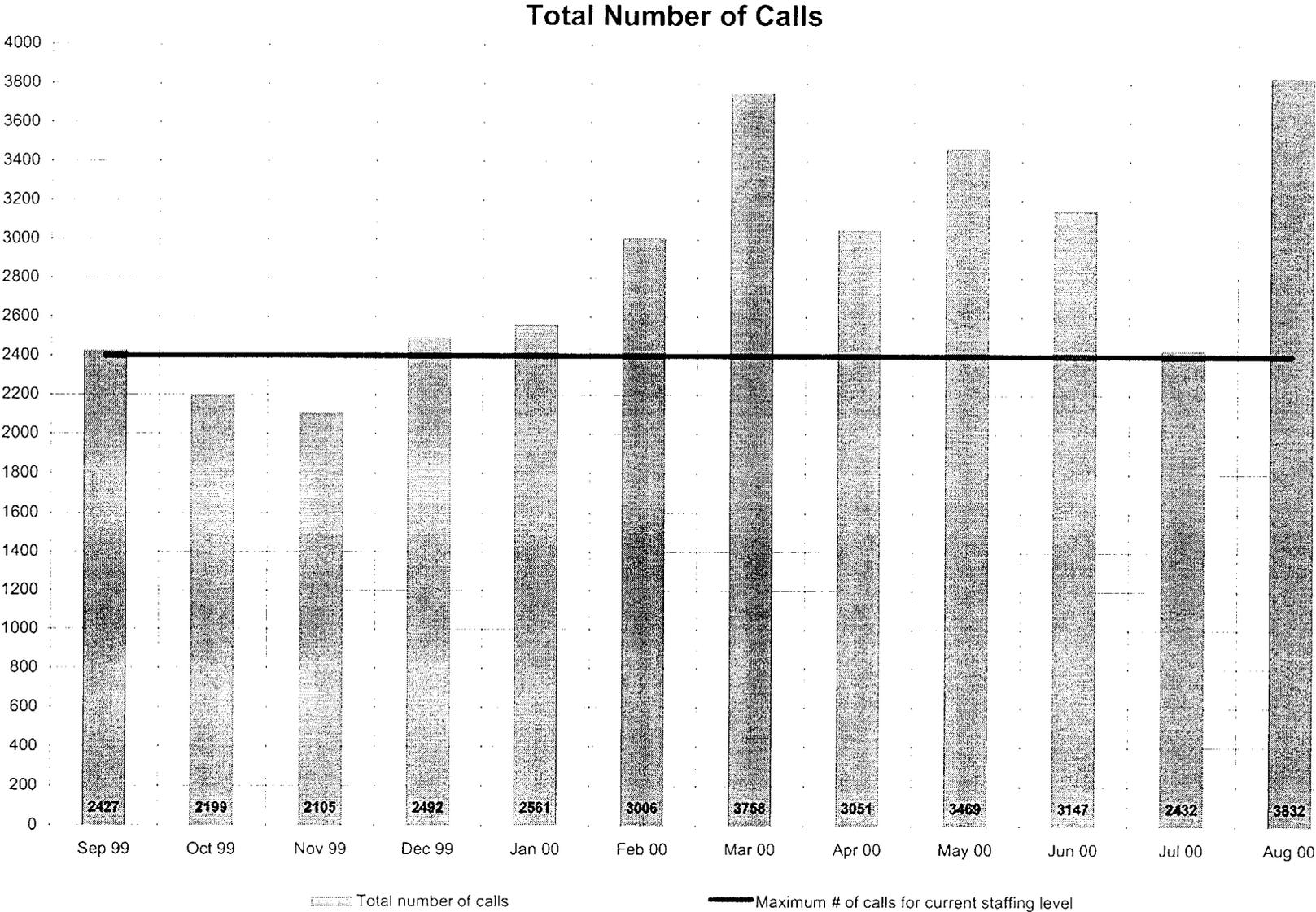
Ticket Type by Department (4/16-4/20)



NOC Monthly Statistics (January, February, and March 2001)

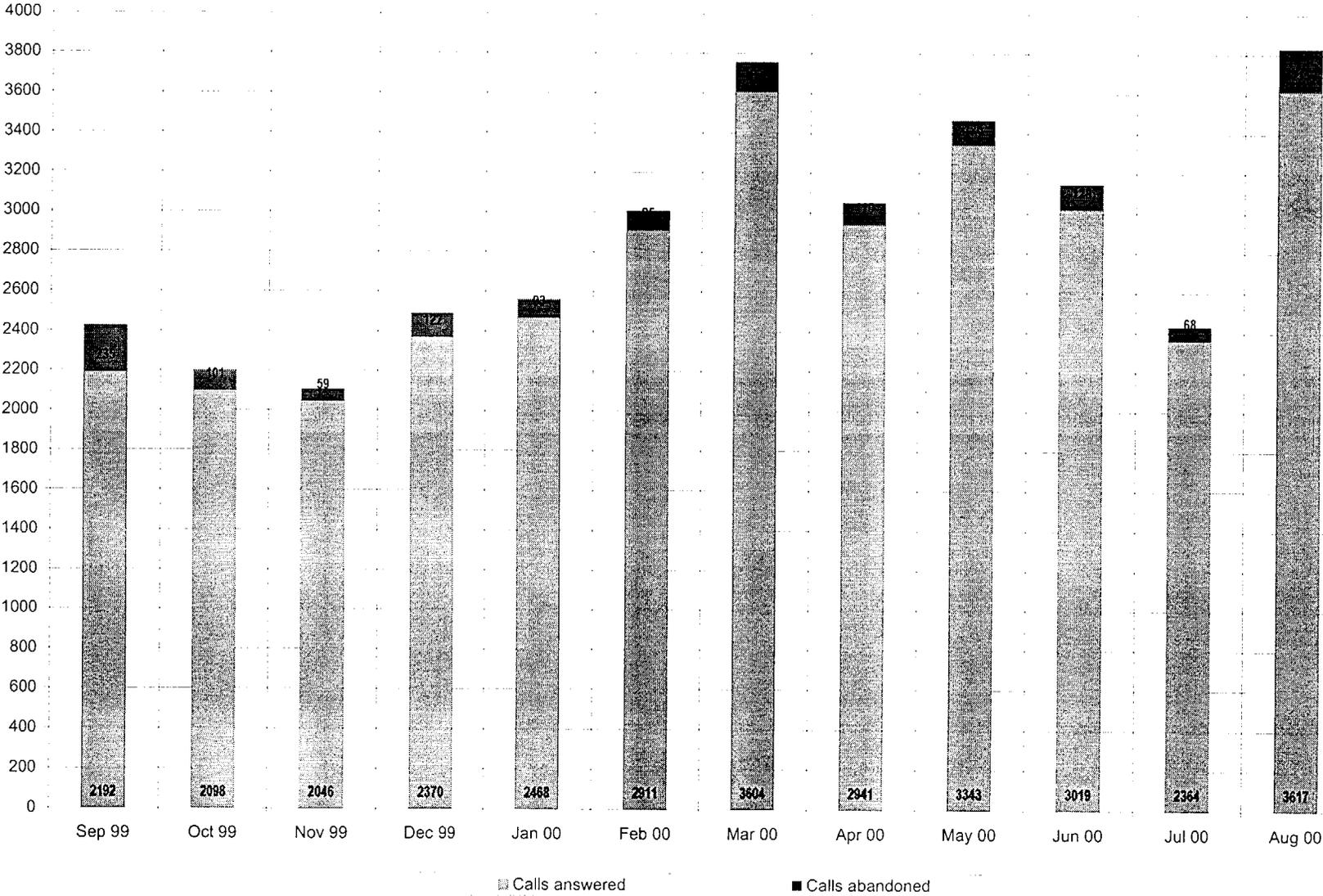


CSC Yearly Call Statistics (September 1999 to August 2000)



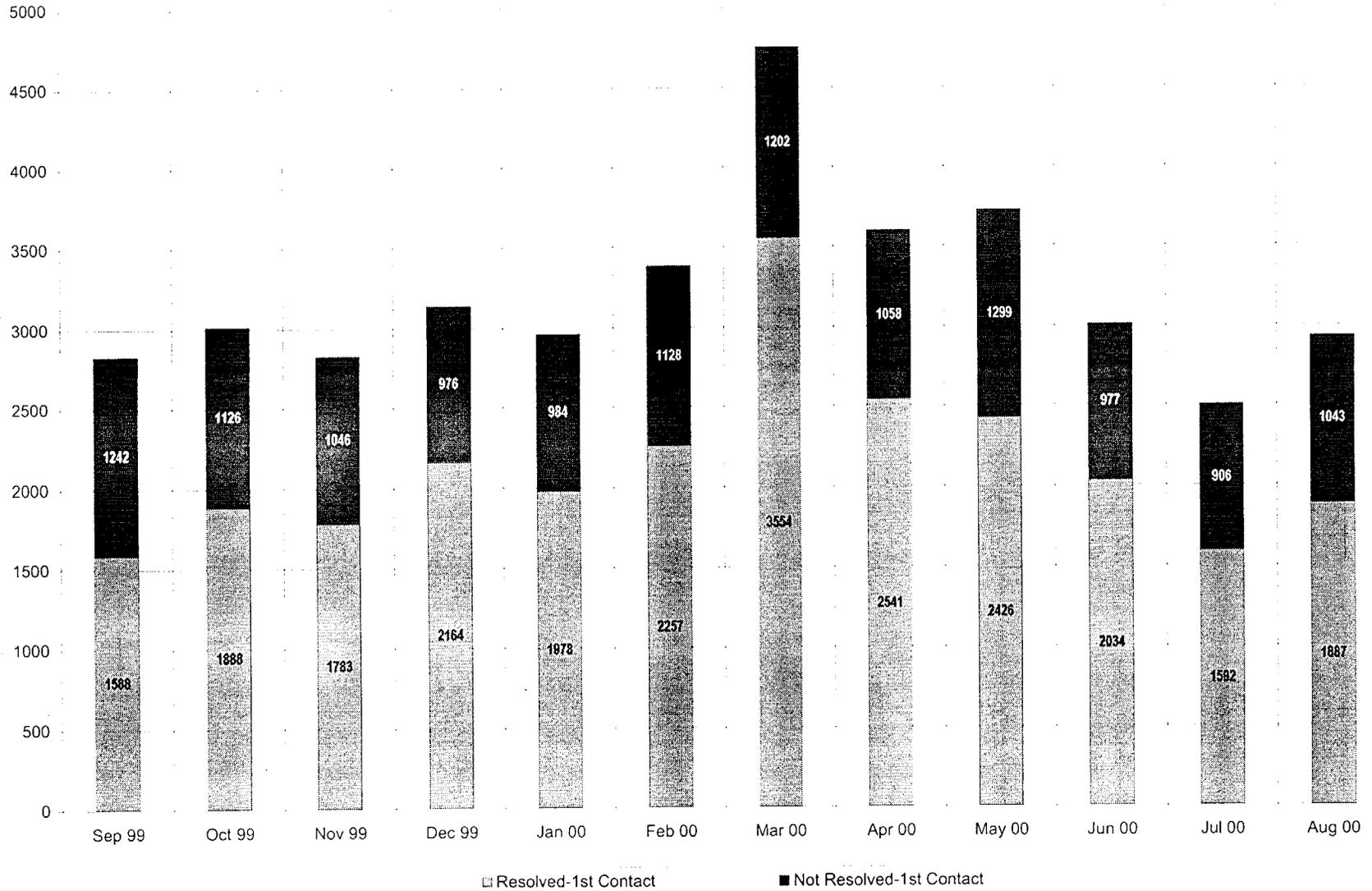
CSC Yearly Call Statistics (September 1999 to August 2000)

Calls Answered and Abandoned

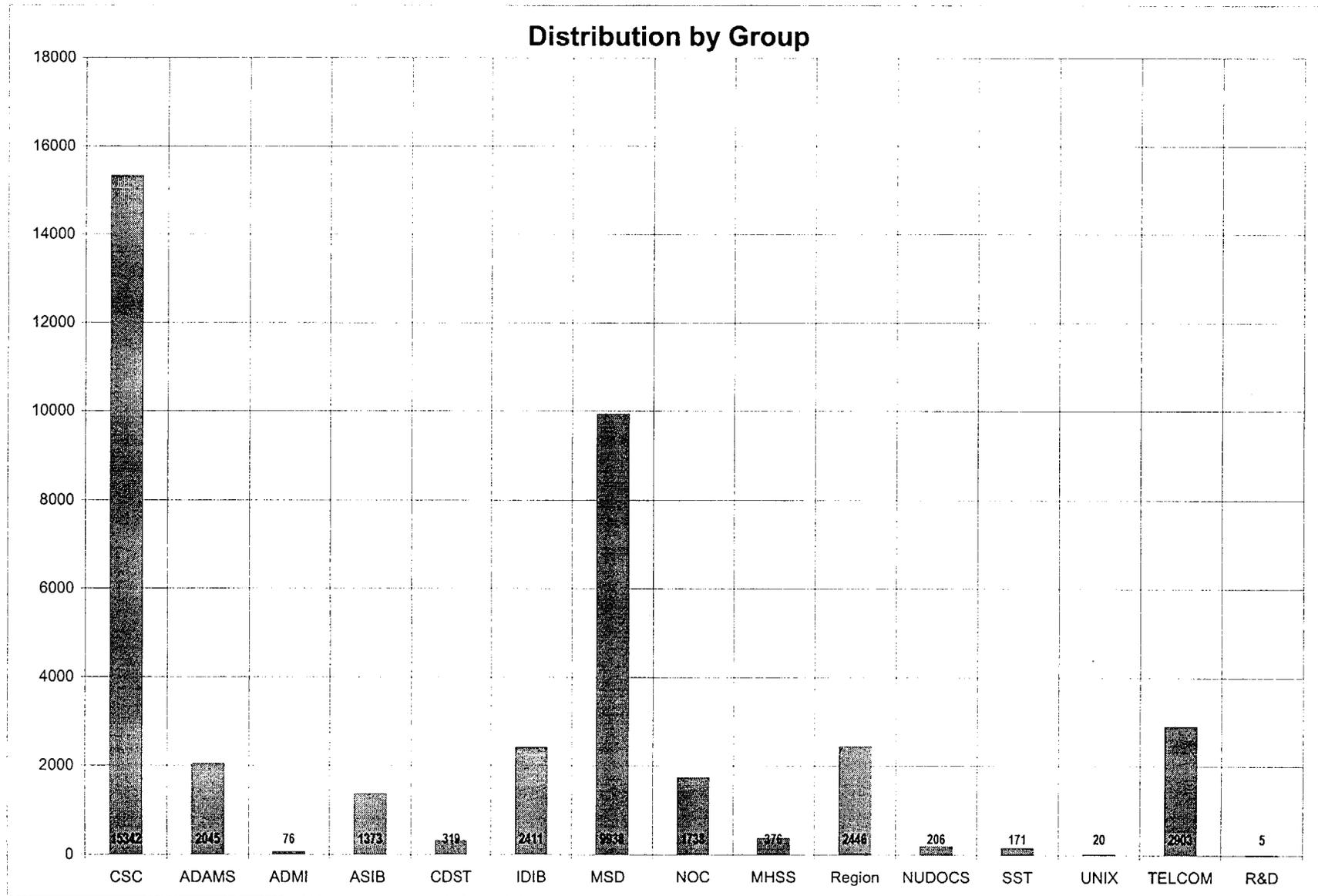


CSC Yearly Ticket Statistics (September 1999 to August 2000)

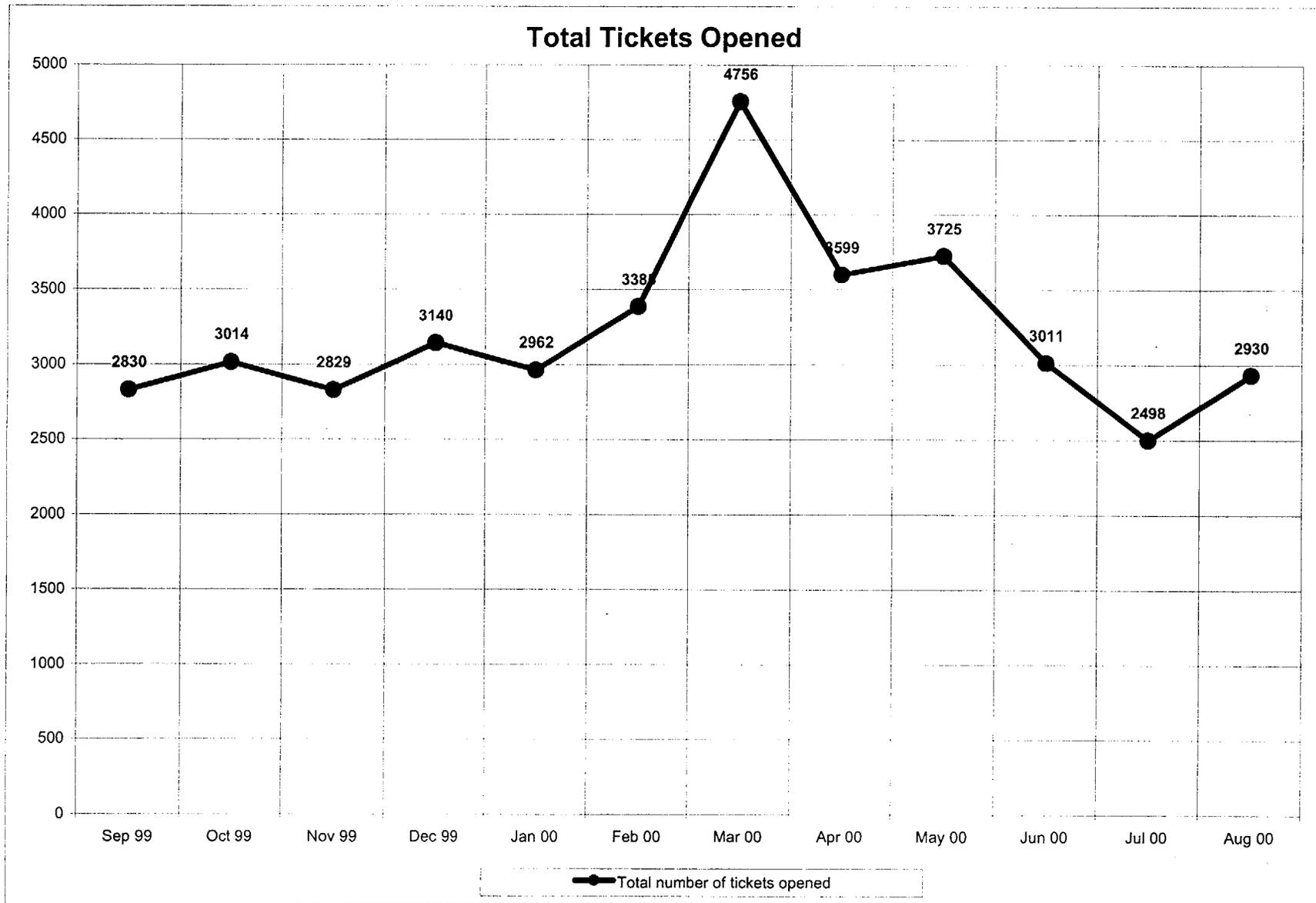
First Level Resolution



CSC Yearly Ticket Statistics (September 1999 to August 2000)



CSC Yearly Ticket Statistics (September 1999 to August 2000)



OTHER NRC SUPPORTED APPLICATIONS

DESKTOP (Detailed breakout in hyperlink)

- NT 4.0 SP5
- Novell 4.71 client
- Norton Anti-Virus 7.02
- Corel Suite 8.0 (WP, Quattro Pro, Presentations)
- GROUPWISE 5.5.3
- Informs 4.3
- Netscape Communicator 4.7
- DiskKeeper 3.0
- QuickTime 3.0
- Adobe Acrobat 4.05c
- CITRIX

Agency Wide Production Application

- ADAMS 3.3.1
- STARFIRE (Report daily time)
- Sybase
- MS SQL
- Tuxedo
- People Soft

File, Mail, App Servers

- NT 4.0 SP5
- Novell NetWare 4.2, SP8A
- DS version 6.09
- Groupwise 5.5.4
- ARCServe6
- Norton AntiVirus Corporate Edition 7.02ce
- ManageWise 2.6
- NetPro DS Analyzer and DSExpert 3.0

High Performance Computing Environment

- UNIX
- Linux
- Scientific Codes

Other Supported Agency Applications (see hyperlink for more detail)

- MS Office Professional (Word, Access, Excel, Powerpoint)
- MS Front Page
- NEXIC
- Visio
- Internet Explorer

Other Supported Agency Applications ([see hyperlink for more detail](#))

- MS Office Professional (Word, Access, Excel, Powerpoint)
- MS Front Page
- NEXIC
- Visio
- Internet Explorer

Name	Location	Size	Product Name
ADAMSCustomCVLEditor.exe	C:\ADAMS\Custom	56KB	ADAMS Custom CVL Editor
ADAMSDistUtil.exe	C:\ADAMS\Custom	584KB	ADMRIDS
ADAMSDM.exe	C:\ADAMS\Custom	72KB	ADAMS Document Manager
ADAMSFInd.exe	C:\ADAMS\Custom	116KB	ADAMS Find Application
ADAMSFMDispTool.exe	C:\ADAMS\Custom	68KB	ADAMS FM Reports Object
ADAMSFMReports.exe	C:\ADAMS\Custom	88KB	ADAMS FM Reports Object
ADAMSFMViewer.exe	C:\ADAMS\Custom	28KB	ADAMS Document Viewer
ADAMSGWLookUp.exe	C:\ADAMS\Custom	24KB	ADAMSGWLookUp Object
ADAMSIntegration.exe	C:\ADAMS\Custom	40KB	ADAMS Integration Object
ADAMSMergeData.exe	C:\ADAMS\Custom	68KB	ADAMS MergeData Object
ADAMSORPCClientNotify.exe	C:\ADAMS\Custom	44KB	ADAMS ORPCClientNotify Application
ADAMSORPQViewer.exe	C:\ADAMS\Custom	48KB	ADAMS ORP Queue Viewer
ADAMSPackageConvert.exe	C:\ADAMS\Custom	52KB	ADAMS Package Conversion Utility
ADAMSPackageViewer.exe	C:\ADAMS\Custom	28KB	ADAMS Package Viewer
ADAMSProfileValidationEditor.exe	C:\ADAMS\Custom	92KB	ADAMS ProfileValidation Editor
ADAMSPublicRulesEditor.exe	C:\ADAMS\Custom	80KB	ADAMSPublicRules
ADAMSRepRestoreUtility.exe	C:\ADAMS\Custom	40KB	ADAMSRepBackup
ADAMSSettingsUtility.exe	C:\ADAMS\Custom	68KB	ADANSSettingUtility Object

ADAMSView.exe	C:\ADAMS\Custom	324KB	ADAMS View
ADAMSViewer.exe	C:\ADAMS\Custom	28KB	ADAMS Document Viewer
AUDLVR32.EXE	C:\ADAMS\FileNET\Ensemble	29KB	
AUOPEN32.EXE	C:\ADAMS\FileNET\Ensemble	29KB	
AUTH32.EXE	C:\ADAMS\FileNET\Ensemble	473KB	Ensemble Application
ENAGNT32.EXE	C:\ADAMS\FileNET\Ensemble	71KB	Ensemble Application
ENGRPH32.EXE	C:\ADAMS\FileNET\Ensemble	14KB	Ensemble Application
ENMEM.EXE	C:\ADAMS\FileNET\Ensemble	10KB	
ENMSRV32.EXE	C:\ADAMS\FileNET\Ensemble	42KB	Ensemble Application
ENPVW16.EXE	C:\ADAMS\FileNET\Ensemble	10KB	
ENROLE32.EXE	C:\ADAMS\FileNET\Ensemble	90KB	Ensemble Application
ENSCAN32.EXE	C:\ADAMS\FileNET\Ensemble	31KB	ENSCAN Application
ENSDLV32.EXE	C:\ADAMS\FileNET\Ensemble	33KB	Ensemble Application
ENSRUN32.EXE	C:\ADAMS\FileNET\Ensemble	247KB	Ensemble Application
ENSWFC32.EXE	C:\ADAMS\FileNET\Ensemble	89KB	Ensemble Application
ENXFRM32.EXE	C:\ADAMS\FileNET\Ensemble	70KB	Ensemble Application
ESP32.EXE	C:\ADAMS\FileNET\Ensemble	140KB	Ensemble Application
EWFOLE32.EXE	C:\ADAMS\FileNET\Ensemble	67KB	Ensemble Application
EXDLVR32.EXE	C:\ADAMS\FileNET\Ensemble	59KB	Ensemble Application
GW16.EXE	C:\ADAMS\FileNET\Ensemble	58KB	Ensemble Application
GWINST.EXE	C:\ADAMS\FileNET\Ensemble	29KB	
STATUS32.EXE	C:\ADAMS\FileNET\Ensemble	320KB	Ensemble Application
VER32.EXE	C:\ADAMS\FileNET\Ensemble	21KB	Version Shower
WFLMGR32.EXE	C:\ADAMS\FileNET\Ensemble	17KB	Ensemble Application
STATDISP.EXE	C:\ADAMS\FileNET\Ensemble\WFStats	17KB	StatDisp

STATXLS.EXE	C:\ADAMS\FileNET\Ensemble\WFStats	17KB	StatXls
FnLCache.exe	C:\ADAMS\FileNET\IDM	135KB	IDM
fnlogspy.exe	C:\ADAMS\FileNET\IDM	114KB	FNLOGSPY Application
fnlogsvr.exe	C:\ADAMS\FileNET\IDM	356KB	FNLOGSVR Application
fnlogvwr.exe	C:\ADAMS\FileNET\IDM	120KB	FileNET Log Viewer Application
FnReg.exe	C:\ADAMS\FileNET\IDM	17KB	FnReg Application
FnSysMgr.exe	C:\ADAMS\FileNET\IDM	28KB	FNSYSMGR Dynamic Link Library
Fntrcadm.exe	C:\ADAMS\FileNET\IDM	100KB	FNTRCADM Application
IDMCfg.exe	C:\ADAMS\FileNET\IDM	135KB	IDM Configure Application
IDMLaunch.exe	C:\ADAMS\FileNET\IDM	26KB	IDMLaunch
IDMView.exe	C:\ADAMS\FileNET\IDM	632KB	Viewer Application
MSG.EXE	C:\ADAMS\FileNET\IDM	52KB	
Npver.exe	C:\ADAMS\FileNET\IDM	37KB	Version Query Application
oscs.exe	C:\ADAMS\FileNET\IDM	31KB	WorkFlow Application Libraries
PAGEHDR.EXE	C:\ADAMS\FileNET\IDM	29KB	
setbrows.exe	C:\ADAMS\FileNET\IDM	5KB	
wal_ipc.exe	C:\ADAMS\FileNET\IDM	113KB	WorkFlow Application Libraries
spping32.exe	C:\ADAMS\FileNET\Shared	35KB	
icrsrv32.exe	C:\ADAMS\Watermark\Client	948KB	TextBridge API
aspiinst.exe	C:\ADAMS\Watermark\Client\temp	25KB	
wmappndx.exe	C:\ADAMS\Watermark\Client\temp	33KB	WMAPPNDX Application
wnl.exe	C:\ADAMS\Watermark\Client\temp	21KB	
wmcred.EXE	C:\ADAMS\Watermark\Client	5KB	
wmexplor.EXE	C:\ADAMS\Watermark\Client	186KB	Watermark Workspace
wmstky.EXE	C:\ADAMS\Watermark\Client	80KB	
wmwspace.EXE	C:\ADAMS\Watermark\Client	186KB	Watermark Workspace
atiplay.exe	C:\ati\atidesk	1,041KB	ATI Multimedia Player

ATI Multimedia Player	45KB	C:\ati\atidesk		atsched.exe
Microsoft® Visual Basic for Windows	27KB	C:\DRIVERS\APM		AMADMIN.EXE
Microsoft® Visual Basic for Windows	58KB	C:\DRIVERS\APM		SETUP.EXE
PC Card Setup	33KB	C:\DRIVERS\APM		SUSPEND.EXE
PC Card Setup	140KB	C:\DRIVERS\APM		UNINSTL.EXE
Ensoniq Mixer Wizard NT Installation	227KB	C:\DRIVERS\AUDIO\ENSONIQ.NT		ENSMIX32.EXE
Ensoniq Mixer Starter	296KB	C:\DRIVERS\AUDIO\ENSONIQ.NT		NTWIZARD.EXE
Ensoniq Mixer	22KB	C:\DRIVERS\AUDIO\ENSONIQ.NT		STARTER.EXE
Ensoniq Mixer	437KB	C:\DRIVERS\AUDIO\ENSONIQ.NT\UPDATE		SETUPPEX.EXE
Ensoniq Mixer	21KB	C:\DRIVERS\AUDIO\MAESTRO2		ESSAPM.EXE
InstallShield®	59KB	C:\DRIVERS\AUDIO\MAESTRO2		SETUP.EXE
InstallShield®	9KB	C:\DRIVERS\AUDIO\MAESTRO2		_ISDEL.EXE
Sound Blaster AWE	270KB	C:\DRIVERS\AUDIO\SB_16-64		AWECP32.EXE
Sound Blaster AWE	949KB	C:\DRIVERS\AUDIO\SB_16-64		AWENT40.EXE
UPDPNPNT	24KB	C:\DRIVERS\AUDIO\SB_16-64		UPDPNPNT.EXE
Intel 825xDel	133KB	C:\DRIVERS\NT4_DOCK		INSTAPI.EXE
Intel(R) PROMonitor	29KB	C:\DRIVERS\NT4_DOCK\NDIS\INTEL		PROMON.EXE
Microsoft® Visual Basic for Windows	86KB	C:\DRIVERS\NT4_DOCK\NDIS\INTEL		SETUP.EXE
Microsoft® Visual Basic for Windows	58KB	C:\DRIVERS\NT4_DOCK		SETUP.EXE
PC Card Setup	10KB	C:\DRIVERS\NT4_DOCK		SETUP16.EXE
PC Card Setup	127KB	C:\DRIVERS\NT4_DOCK		UNINSTL.EXE
Setup	72KB	C:\DRIVERS\PRINT\J55\DISK1		SETUP.EXE
InstallShield	45KB	C:\DRIVERS\SYBASE1\INSTALL		SETUP.EXE
InstallShield	8KB	C:\DRIVERS\SYBASE1\INSTALL		_ISDEL.EXE
NRR	37KB	C:\DRIVERS\SYBASE1		SETUP.EXE
InstallShield®	59KB	C:\DRIVERS\VIDEO\ATI		SETUP.EXE
28KB		C:\DRIVERS\VIDEO\ATI		STARTHTM.EXE

_ISDEL.EXE	C:\DRIVERS\VIDEO\ATI	9KB	InstallShield®
SETUP.EXE	C:\DRIVERS\VIDEO\MATROX	318KB	Matrox Graphics Inc. _instpgm
_isdell.exe	C:\DRIVERS\VIDEO\RAGEAGP\NT4_R128.ZIP	9KB	
setup.exe	C:\DRIVERS\VIDEO\RAGEAGP\NT4_R128.ZIP	59KB	
SETUP.EXE	C:\DRIVERS\VIDEO\RAGEAGP	59KB	InstallShield®
_ISDEL.EXE	C:\DRIVERS\VIDEO\RAGEAGP	9KB	InstallShield®
SETUP.EXE	C:\DRIVERS\VIDEO\SAVAGE4	43KB	
ScanFat.exe	C:\EXECISOFT\DISKEEP\ANALYZE	89KB	
ScanNtfs.exe	C:\EXECISOFT\DISKEEP\ANALYZE	108KB	
Connect.exe	C:\EXECISOFT\DISKEEP	19KB	
Control.exe	C:\EXECISOFT\DISKEEP	286KB	Executive Software Controller
DkFat.exe	C:\EXECISOFT\DISKEEP\DEFRAG	102KB	
DkNtfs.exe	C:\EXECISOFT\DISKEEP\DEFRAG	105KB	
DkSched.exe	C:\EXECISOFT\DISKEEP	45KB	Executive Software DkSched
DkService.exe	C:\EXECISOFT\DISKEEP	16KB	
DkWork.exe	C:\EXECISOFT\DISKEEP	182KB	Diskeeper
Uninstall.exe	C:\EXECISOFT\DISKEEP	23KB	
ISQL.EXE	C:\MSSQL\BINN	90KB	Microsoft SQL Server
ISQLW.EXE	C:\MSSQL\BINN	78KB	Microsoft SQL Server
MAKEPIPE.EXE	C:\MSSQL\BINN	25KB	Microsoft SQL Server
READPIPE.EXE	C:\MSSQL\BINN	26KB	Microsoft SQL Server
REGFONT.EXE	C:\MSSQL\BINN	8KB	
REGSVR32.EXE	C:\MSSQL\BINN	24KB	Microsoft® Visual C++
WINDBVER.EXE	C:\MSSQL\BINN	41KB	Microsoft SQL Server
REMOVELAUNCHER.EXE	C:\NGN\COREL\APPMAN\SETUP	53KB	PerfectFit Installation System
DVSETUP7.EXE	C:\NGN\COREL\ENVOY	202KB	Dvsetup7.exe
ENVOY7.EXE	C:\NGN\COREL\ENVOY	1,905KB	Envoy 7 For Windows 95
EVYGW7.EXE	C:\NGN\COREL\ENVOY\SYSTEM	46KB	Envoy 7 For Windows 95
CDRCONV.EXE	C:\NGN\COREL\PROGRAMS\CONVERT	2,782KB	CorelDRAW (TM)
DMODELER.EXE	C:\NGN\COREL\PROGRAMS	771KB	
PFIM80.EXE	C:\NGN\COREL\PROGRAMS	104KB	PerfectFit 32-Bit

PFIS80.EXE	C:\NGN\COREL\PROGRAMS	58KB	PerfectFit 32-Bit
Pfppop80.exe	C:\NGN\COREL\PROGRAMS	302KB	PerfectFit 32-Bit
PFREG.EXE	C:\NGN\COREL\PROGRAMS	89KB	
PRWIN8.EXE	C:\NGN\COREL\PROGRAMS	3,178KB	Presentations for Windows
PS80.EXE	C:\NGN\COREL\PROGRAMS	611KB	PerfectFit 32-Bit
QFINDER.EXE	C:\NGN\COREL\PROGRAMS	58KB	PerfectFit 32-Bit
QFSCHD80.EXE	C:\NGN\COREL\PROGRAMS	58KB	PerfectFit 32-Bit
QPW.EXE	C:\NGN\COREL\PROGRAMS	4,438KB	Quattro Pro for Windows
SCRBOOK.EXE	C:\NGN\COREL\PROGRAMS	91KB	Scrpbook for Windows
PR8_HTML.EXE	C:\NGN\COREL\PROGRAMS\TOOLS	515KB	Presentations for Windows
RTSETUP.EXE	C:\NGN\COREL\PROGRAMS\TOOLS	228KB	Presentations for Windows
SELFEXEC.EXE	C:\NGN\COREL\PROGRAMS\TOOLS	184KB	Presentations for Windows
SHOW.EXE	C:\NGN\COREL\PROGRAMS\TOOLS	461KB	Presentations for Windows
SHOW31.EXE	C:\NGN\COREL\PROGRAMS\TOOLS	110KB	Presentations for Windows
UA80.EXE	C:\NGN\COREL\PROGRAMS	132KB	PerfectFit 32-Bit
WPD8REST.EXE	C:\NGN\COREL\PROGRAMS	338KB	wpd8rest Application
WPWIN8.EXE	C:\NGN\COREL\PROGRAMS	4,072KB	WordPerfect for Windows
CRLAB.EXE	C:\NGN\COREL\SHARED\ADDRESS	50KB	WordPerfect for Windows
EQNEDT32.EXE	C:\NGN\COREL\SHARED\EQUATION	482KB	Corel Equation Editor
BDEADMIN.EXE	C:\NGN\COREL\SHARED\IDAPI	893KB	
REFCNTR.EXE	C:\NGN\COREL\SHARED\REFCNTR	390KB	
TEXTART.EXE	C:\NGN\COREL\SHARED\TEXTART	418KB	TextArt

ADDRBOOK.EXE	C:\NGN\GroupWise	51KB	Novell GroupWise 5 Address Book
CPAdmin.exe	C:\NGN\GroupWise	29KB	
cplace.exe	C:\NGN\GroupWise	226KB	Conversation Place
GrpWise.exe	C:\NGN\GroupWise	3,936KB	GroupWise
GWNLI.EXE	C:\NGN\GroupWise	21KB	
htrsetup.exe	C:\NGN\GroupWise	13KB	GroupWise 'Hit the Road' setup
Notify.exe	C:\NGN\GroupWise	187KB	Notify
FFWIN.EXE	C:\NGN\INFORMS	26KB	
FFWIN41.EXE	C:\NGN\INFORMS	625KB	
GSC.EXE	C:\NGN\INFORMS	763KB	Novell GroupWare Customer Support Information
GWMH.EXE	C:\NGN\INFORMS	177KB	
INDIAG.EXE	C:\NGN\INFORMS	13KB	
INDIAG42.EXE	C:\NGN\INFORMS	532KB	Novell InForms Diagnostics
MAPIMHAP.EXE	C:\NGN\INFORMS	167KB	
NOVREGED.EXE	C:\NGN\INFORMS	476KB	Novell Registry Editor
PROXY16.EXE	C:\NGN\INFORMS	43KB	
PROXYDDE.EXE	C:\NGN\INFORMS	107KB	
SUPINFO.EXE	C:\NGN\INFORMS	178KB	
123WIN.EXE	C:\NGN\SHARED\WPC20	65KB	
BIFED20.EXE	C:\NGN\SHARED\WPC20	36KB	PerfectFit 16-bit
DTWIN20.EXE	C:\NGN\SHARED\WPC20	85KB	
EXWIN.EXE	C:\NGN\SHARED\WPC20	65KB	
GKWIN60.EXE	C:\NGN\SHARED\WPC20	209KB	Grammatik
BDECFG.EXE	C:\NGN\SHARED\WPC20\IDAPI	353KB	
KICKOFF.EXE	C:\NGN\SHARED\WPC20	34KB	PerfectFit 16-bit
MCVWIN.EXE	C:\NGN\SHARED\WPC20	416KB	
MCWIN20.EXE	C:\NGN\SHARED\WPC20	120KB	PerfectFit 16-bit
MFWIN20.EXE	C:\NGN\SHARED\WPC20	155KB	PerfectFit 16-bit
MXWIN20.EXE	C:\NGN\SHARED\WPC20	151KB	PerfectFit 16-bit

POSETUP.EXE	C:\NGN\SHARED\WP20	1,211KB	
QFWIN20.EXE	C:\NGN\SHARED\WP20	193KB	WP Shared Code
SETUP.EXE	C:\NGN\SHARED\WP20	9KB	
SPWIN20.EXE	C:\NGN\SHARED\WP20	68KB	PerfectFit 16-bit
THWIN20.EXE	C:\NGN\SHARED\WP20	39KB	PerfectFit 16-bit
WAIT.EXE	C:\NGN\SHARED\WP20	5KB	
WPBT61.EXE	C:\NGN\SHARED\WP20	12KB	
WPRINT20.EXE	C:\NGN\SHARED\WP20	313KB	WordPerfect for Windows
ADMIN.EXE	C:\NTAGENT	350KB	
COMPRESS.EXE	C:\NTAGENT	89KB	Microsoft(R) Windows NT(TM) Operating System
NTAGENT.EXE	C:\NTAGENT	324KB	ARCserve Win32 Client Agent
NTAGUNIN.EXE	C:\NTAGENT	139KB	ntagunin Application
NTAGUNSS.EXE	C:\NTAGENT	138KB	Ntagunss Application
UNINST.EXE	C:\NTAGENT	293KB	InstallShield uninstaller
AcroRd32.exe	C:\Program Files\ACROBAT3\READER	2,280KB	Adobe Acrobat
ACRORD32.EXE	C:\Program Files\ADOBE\Acrobat 4.0\READER	2,280KB	Adobe Acrobat
REMOVE.EXE	C:\Program Files\Common Files\Microsoft Shared\DAO	25KB	
SEVINST.EXE	C:\Program Files\Common Files\Syantec Shared	372KB	Syantec Core Technology Infoseek Corporation Quickseek
Quickseek.exe	C:\Program Files\INFOSEEK\Quickseek	24KB	
backlog.exe	C:\Program Files\NAVNT	26KB	
defwatch.exe	C:\Program Files\NAVNT	28KB	Norton AntiVirus
dwhwizrld.exe	C:\Program Files\NAVNT	380KB	Norton AntiVirus
ldvpreq.exe	C:\Program Files\NAVNT	28KB	Norton AntiVirus
luawrap.exe	C:\Program Files\NAVNT	32KB	
navustub.exe	C:\Program Files\NAVNT	28KB	

rtvscan.exe	C:\Program Files\NAVNT	372KB	Norton Antivirus
vpc32.exe	C:\Program Files\NAVNT	204KB	Norton Antivirus
vpdfn_lu.exe	C:\Program Files\NAVNT	28KB	Norton Antivirus
vptray.exe	C:\Program Files\NAVNT	48KB	Norton Antivirus
AIM.EXE	C:\Program Files\NETSCAPE\PROGRAM\AIM	10KB	AOL Instant Messenger (SM)
AIMAUTO.EXE	C:\Program Files\NETSCAPE\PROGRAM\AIMAUTO	153KB	AIMAUTO
IMPORT32.EXE	C:\Program Files\NETSCAPE\PROGRAM	35KB	NSImportApp Application
NETSCAPE.EXE	C:\Program Files\NETSCAPE\PROGRAM	5,401KB	NETSCAPE
NSNOTIFY.EXE	C:\Program Files\NETSCAPE\PROGRAM	64KB	Netescape Communications nnotify
SENDTO32.EXE	C:\Program Files\NETSCAPE\PROGRAM	61KB	
TALKBACK.EXE	C:\Program Files\NETSCAPE\PROGRAM	295KB	Talkback
WINAMP.EXE	C:\Program Files\NETSCAPE\WINAMP	844KB	Winamp
NETQUERY.EXE	C:\Program Files\ONNET32	250KB	PC/TCP OnNet32
NETTIME.EXE	C:\Program Files\ONNET32	40KB	PC/TCP OnNet32
OPNSCRPT.EXE	C:\Program Files\ONNET32	354KB	PC/TCP OnNet32
OPNSDLGE.EXE	C:\Program Files\ONNET32	567KB	OPEN Script
OPNSRUN.EXE	C:\Program Files\ONNET32	18KB	
RETRV32.EXE	C:\Program Files\ONNET32	61KB	PC/TCP OnNet32
RUTIL.EXE	C:\Program Files\ONNET32	92KB	PC/TCP OnNet32
ENGINE.EXE	C:\Program Files\ONNET32\TNBLUE	226KB	ENGINE Application
FTPVRT.EXE	C:\Program Files\ONNET32\TNBLUE	112KB	RTITBL
KEYMAP.EXE	C:\Program Files\ONNET32\TNBLUE	62KB	Tnblue KEYMAP Application
TNBLUE.EXE	C:\Program Files\ONNET32\TNBLUE	322KB	PC/TCP OnNet32
TNVT.EXE	C:\Program Files\ONNET32\TNVT	986KB	PC/TCP OnNet32

UNINST.EXE	C:\Program Files\ONNET32	88KB	PC/TCP OnNet32
UPGRADE.EXE	C:\Program Files\ONNET32	42KB	
WFTP.EXE	C:\Program Files\ONNET32	575KB	PC/TCP OnNet32
PPVIEW32.EXE	C:\Program Files\PowerPoint Viewer	1,393KB	
SETUP.EXE	C:\Program Files\PowerPoint Viewer\setup	345KB	Microsoft App-wide Setup for Windows
MoviePlayer.exe	C:\Program Files\QuickTime	606KB	Apple Computer, Inc. MoviePlayer Application
PictureViewer.exe	C:\Program Files\QuickTime	151KB	Apple Computer, Inc. PictureViewer Application
QTInfo.exe	C:\Program Files\QuickTime	278KB	QuickTime
LUAll.exe	C:\Program Files\SYMANTEC\LiveUpdate	96KB	LiveUpdate
Uninst.exe	C:\Program Files\SYMANTEC\LiveUpdate	76KB	LiveUpdate
wangimg.exe	C:\Program Files\Windows NT\Accessories\ImageVue	418KB	Imaging for Windows NT
WORDPAD.EXE	C:\Program Files\Windows NT\Accessories	200KB	Microsoft(R) Windows NT(TM) Operating System
dialer.exe	C:\Program Files\Windows NT	42KB	Microsoft(R) Windows NT(TM) Operating System
HYPERTRM.EXE	C:\Program Files\Windows NT	10KB	Microsoft(R) Windows NT(TM) Operating System
EXCHNG32.EXE	C:\Program Files\Windows NT\Windows Messaging	28KB	Microsoft(R) Windows NT(TM) Operating System
SCANPST.EXE	C:\Program Files\Windows NT\Windows Messaging	234KB	Microsoft(R) Windows NT(TM) Operating System
Report Daily Time.exe	C:\PS	369KB	Report Daily Time
BCP.EXE	C:\SQL\BIN	60KB	
DEFNCPY.EXE	C:\SQL\BIN	42KB	
DSEdit.EXE	C:\SQL\BIN	381KB	DSEdit Application
DSYBPING.EXE	C:\SQL\BIN	18KB	
ISQL.EXE	C:\SQL\BIN	41KB	
NLLWPTCP.EXE	C:\SQL\BIN	28KB	
NLNMPIPE.EXE	C:\SQL\BIN	17KB	
NLNULL.EXE	C:\SQL\BIN	11KB	
OCSCFG.EXE	C:\SQL\BIN	223KB	OCSCFG

			Application
PING32.EXE	C:\SQL\BIN	7KB	
SQLADV.EXE	C:\SQL\BIN	597KB	Sybase SQL Advantage
SQLEDIT.EXE	C:\SQL\BIN	65KB	
SYBENV32.EXE	C:\SQL\BIN	6KB	
SYBPING.EXE	C:\SQL\BIN	18KB	
WBCP.EXE	C:\SQL\BIN	73KB	
WDEFNCPY.EXE	C:\SQL\BIN	49KB	
WDLLVERS.EXE	C:\SQL\BIN	36KB	
WDSEDIT.EXE	C:\SQL\BIN	200KB	
WISQL.EXE	C:\SQL\BIN	80KB	
WOCSCFG.EXE	C:\SQL\BIN	125KB	
WSYBPING.EXE	C:\SQL\BIN	23KB	
CD32.EXE	C:\WINDOWS	619KB	
CD32405.EXE	C:\WINDOWS	620KB	
EXPLORER.EXE	C:\WINDOWS	232KB	Microsoft(R) Windows NT(TM) Operating System
IEHELP.EXE	C:\WINDOWS	148KB	
IsUninst.exe	C:\WINDOWS	300KB	InstallShield® unInstaller
LD32404.EXE	C:\WINDOWS	621KB	
NOTEPAD.EXE	C:\WINDOWS	45KB	Microsoft(R) Windows NT(TM) Operating System
REGEDIT.EXE	C:\WINDOWS	71KB	Microsoft(R) Windows NT(TM) Operating System
REGTLIB.EXE	C:\WINDOWS	30KB	
ST5UNST.EXE	C:\WINDOWS	70KB	Microsoft® Visual Basic for Windows
loginw31.exe	C:\WINDOWS\system	5KB	
WOWPOST.EXE	C:\WINDOWS\system	5KB	EZ-SCSI
append.exe	C:\WINDOWS\system32	11KB	
ARP.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
ASDSCSVC.EXE	C:\WINDOWS\system32	127KB	
at.exe	C:\WINDOWS\system32	28KB	Microsoft(R) Windows NT(TM) Operating System
ati2plab.exe	C:\WINDOWS\system32	51KB	
atiiprxx.exe	C:\WINDOWS\system32	88KB	ATI Graphics Accelerators

atiphexx.exe	C:\WINDOWS\system32	36KB	ATI Technologies, Inc.
atiptaaa.exe	C:\WINDOWS\system32	213KB	ATI Technologies, Inc.
atiptaab.exe	C:\WINDOWS\system32	215KB	ATI Technologies, Inc.
ATSVC.EXE	C:\WINDOWS\system32	23KB	Microsoft(R) Windows NT(TM) Operating System
attrib.exe	C:\WINDOWS\system32	28KB	Microsoft(R) Windows NT(TM) Operating System
AUDITPOL.EXE	C:\WINDOWS\system32	34KB	
AUTOCHK.EXE	C:\WINDOWS\system32	420KB	Microsoft(R) Windows NT(TM) Operating System
AUTOCONV.EXE	C:\WINDOWS\system32	439KB	Microsoft(R) Windows NT(TM) Operating System
AutoFAT.EXE	C:\WINDOWS\system32	176KB	
autofn.exe	C:\WINDOWS\system32	12KB	Microsoft(R) Windows NT(TM) Operating System
AutoNTFS.exe	C:\WINDOWS\system32	182KB	
backup.exe	C:\WINDOWS\system32	36KB	
BOOTOK.EXE	C:\WINDOWS\system32	28KB	Microsoft(R) Windows NT(TM) Operating System
BOOTVRFY.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
CACLS.EXE	C:\WINDOWS\system32	65KB	Microsoft(R) Windows NT(TM) Operating System
CALC.EXE	C:\WINDOWS\system32	96KB	Microsoft(R) Windows NT(TM) Operating System
cdplayer.exe	C:\WINDOWS\system32	85KB	Microsoft(R) Windows NT(TM) Operating System
charmapp.exe	C:\WINDOWS\system32	62KB	Microsoft(R) Windows NT(TM) Operating System
CHKDSK.EXE	C:\WINDOWS\system32	34KB	Microsoft(R) Windows NT(TM) Operating System
CHKNTFS.EXE	C:\WINDOWS\system32	32KB	Microsoft(R) Windows NT(TM) Operating System
cliconfg.exe	C:\WINDOWS\system32	37KB	Microsoft SQL Server Microsoft®

clipbrd.exe	C:\WINDOWS\system32	131KB	Windows(TM) Operating System
clipsrv.exe	C:\WINDOWS\system32	58KB	Microsoft® Windows(TM) Operating System
CLOCK.EXE	C:\WINDOWS\system32	42KB	Microsoft(R) Windows NT(TM) Operating System
CMD.EXE	C:\WINDOWS\system32	204KB	Microsoft(R) Windows NT(TM) Operating System
cmdinfo.exe	C:\WINDOWS\system32	13KB	
comp.exe	C:\WINDOWS\system32	36KB	Microsoft(R) Windows NT(TM) Operating System
COMPACT.EXE	C:\WINDOWS\system32	52KB	Microsoft(R) Windows NT(TM) Operating System
control.exe	C:\WINDOWS\system32	9KB	Microsoft(R) Windows NT(TM) Operating System
CONVERT.EXE	C:\WINDOWS\system32	32KB	Microsoft(R) Windows NT(TM) Operating System
CSRSS.EXE	C:\WINDOWS\system32	8KB	Microsoft(R) Windows NT(TM) Operating System
CSVROOT.EXE	C:\WINDOWS\system32	7KB	Microsoft(R) Windows NT(R) Operating System
DCOMCNFG.EXE	C:\WINDOWS\system32	138KB	Microsoft(R) Windows NT(R) Operating System
DDESHARE.EXE	C:\WINDOWS\system32	33KB	Microsoft(R) Windows NT(TM) Operating System
DDHELP.EXE	C:\WINDOWS\system32	28KB	Microsoft(R) Windows NT(TM) Operating System
debug.exe	C:\WINDOWS\system32	21KB	
DELTREE.EXE	C:\WINDOWS\system32	11KB	
diskperf.exe	C:\WINDOWS\system32	35KB	Microsoft(R) Windows NT(TM) Operating System
DLLHOST.EXE	C:\WINDOWS\system32	12KB	Microsoft(R) Windows NT(TM) Operating System
doskey.exe	C:\WINDOWS\system32	35KB	Microsoft(R) Windows NT(TM) Operating System
DOSX.EXE	C:\WINDOWS\system32	36KB	
DPLAYSVR.EXE	C:\WINDOWS\system32	30KB	Microsoft® DirectX for Windows®
dpmw32.exe	C:\WINDOWS\system32	28KB	

drwatson.exe	C:\WINDOWS\system32	28KB	Microsoft® Windows(TM) Operating System
DRWTSN32.EXE	C:\WINDOWS\system32	66KB	Microsoft(R) Windows NT(TM) Operating System
DSSSIG.EXE	C:\WINDOWS\system32	24KB	Microsoft(R) Windows NT(R) Operating System
edlin.exe	C:\WINDOWS\system32	13KB	
EVENTVWR.EXE	C:\WINDOWS\system32	110KB	Microsoft(R) Windows NT(TM) Operating System
exe2bin.exe	C:\WINDOWS\system32	9KB	
expand.exe	C:\WINDOWS\system32	58KB	Microsoft(R) Windows NT(TM) Operating System
fastopen.exe	C:\WINDOWS\system32	1KB	
fc.exe	C:\WINDOWS\system32	40KB	Microsoft(R) Windows NT(TM) Operating System
find.exe	C:\WINDOWS\system32	30KB	Microsoft(R) Windows NT(TM) Operating System
findstr.exe	C:\WINDOWS\system32	25KB	Microsoft(R) Windows NT(TM) Operating System
FINGER.EXE	C:\WINDOWS\system32	12KB	Microsoft(R) Windows NT(TM) Operating System
FONTVIEW.EXE	C:\WINDOWS\system32	32KB	Microsoft(R) Windows NT(TM) Operating System
forcedos.exe	C:\WINDOWS\system32	23KB	Microsoft(R) Windows NT(TM) Operating System
FTP.EXE	C:\WINDOWS\system32	41KB	Microsoft(R) Windows NT(TM) Operating System
gdi.exe	C:\WINDOWS\system32	21KB	Microsoft® Windows(TM) Operating System
GRPCONV.EXE	C:\WINDOWS\system32	47KB	Microsoft(R) Windows NT(TM) Operating System
Gwshlimp.exe	C:\WINDOWS\system32	13KB	GWCNNIMP Application
gwshlsnd.exe	C:\WINDOWS\system32	13KB	GWCNSND Application
help.exe	C:\WINDOWS\system32	31KB	Microsoft(R) Windows NT(TM) Operating System
HOSTNAME.EXE	C:\WINDOWS\system32	11KB	Microsoft(R) Windows NT(TM) Operating System

inetins.exe	C:\WINDOWS\system32	14KB	Microsoft(R) Windows NT(TM) Operating System
internat.exe	C:\WINDOWS\system32	17KB	Microsoft(R) Windows NT(TM) Operating System
IPCONFIG.EXE	C:\WINDOWS\system32	22KB	Microsoft(R) Windows NT(TM) Operating System
IPROP.EXE	C:\WINDOWS\system32	88KB	OLE PropertySet Implementation Setup
IPXROUTE.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
KILL.EXE	C:\WINDOWS\system32	35KB	Microsoft(R) Windows NT(TM) Operating System
KRNL386.EXE	C:\WINDOWS\system32	84KB	Microsoft® Windows(TM) Operating System
LABEL.EXE	C:\WINDOWS\system32	32KB	Microsoft(R) Windows NT(TM) Operating System
lights.exe	C:\WINDOWS\system32	35KB	Microsoft(R) Windows NT(TM) Operating System
LMREPL.EXE	C:\WINDOWS\system32	85KB	Microsoft(R) Windows NT(TM) Operating System
LOCATOR.EXE	C:\WINDOWS\system32	116KB	Microsoft(R) Windows NT(TM) Operating System
LODCTR.EXE	C:\WINDOWS\system32	20KB	Microsoft(R) Windows NT(TM) Operating System
loginw32.exe	C:\WINDOWS\system32	28KB	Novell Client Login for 32-bit Windows
loginwnt.exe	C:\WINDOWS\system32	28KB	Novell Client Login for 32-bit Windows
LSASS.EXE	C:\WINDOWS\system32	10KB	Microsoft(R) Windows NT(TM) Operating System
MAPISP32.EXE	C:\WINDOWS\system32	10KB	Microsoft(R) Windows NT(TM) Operating System
MAPISRV.R.EXE	C:\WINDOWS\system32	22KB	Microsoft(R) Windows NT(TM) Operating System
MDISP32.EXE	C:\WINDOWS\system32	65KB	Microsoft(R) Windows NT(TM) Operating System
mem.exe	C:\WINDOWS\system32	39KB	
ML3XEC16.EXE	C:\WINDOWS\system32	8KB	Microsoft® Windows(TM)

File Name	Path	Size	Description
			Operating System
mpegunst.exe	C:\WINDOWS\system32	123KB	ATI Video Player
mplay32.exe	C:\WINDOWS\system32	135KB	Microsoft(R) Windows NT(TM) Operating System
mpnotify.exe	C:\WINDOWS\system32	23KB	Microsoft(R) Windows NT(TM) Operating System
mscdexnt.exe	C:\WINDOWS\system32	1KB	
MSPAINT.EXE	C:\WINDOWS\system32	332KB	Microsoft(R) Windows NT(TM) Operating System
MUSRMGR.EXE	C:\WINDOWS\system32	252KB	Microsoft(R) Windows NT(TM) Operating System
NALNTSRV.EXE	C:\WINDOWS\system32	108KB	Novell nalntsrv
nalsrvld.exe	C:\WINDOWS\system32	88KB	Novell nalsrvld
NBTSTAT.EXE	C:\WINDOWS\system32	20KB	Microsoft(R) Windows NT(TM) Operating System
NDDEAGNT.EXE	C:\WINDOWS\system32	14KB	Microsoft(R) Windows NT(TM) Operating System
NDDEAPIR.EXE	C:\WINDOWS\system32	9KB	Microsoft(R) Windows NT(TM) Operating System
NET.EXE	C:\WINDOWS\system32	54KB	Microsoft(R) Windows NT(TM) Operating System
NET1.EXE	C:\WINDOWS\system32	139KB	Microsoft(R) Windows NT(TM) Operating System
NETDDE.EXE	C:\WINDOWS\system32	116KB	Microsoft(R) Windows NT(TM) Operating System
NETDOM.EXE	C:\WINDOWS\system32	77KB	
NETSTAT.EXE	C:\WINDOWS\system32	25KB	Microsoft(R) Windows NT(TM) Operating System
Nwmig.exe	C:\WINDOWS\system32\NetWare\nwmigw2k	24KB	
Setuppw2k.exe	C:\WINDOWS\system32\NetWare\nwmigw2k	24KB	
NHLOADER.EXE	C:\WINDOWS\system32	220KB	Windows NT Server, Enterprise Edition Installer

nlsfunc.exe	C:\WINDOWS\system32	7KB	
notepad.exe	C:\WINDOWS\system32	45KB	Microsoft(R) Windows NT(TM) Operating System
NSLOOKUP.EXE	C:\WINDOWS\system32	65KB	Microsoft(R) Windows NT(TM) Operating System
NTBACKUP.EXE	C:\WINDOWS\system32	695KB	Microsoft(R) Windows NT(TM) Operating System
NTOSKRNL.EXE	C:\WINDOWS\system32	907KB	Microsoft(R) Windows NT(TM) Operating System
NTRIGHT1.EXE	C:\WINDOWS\system32	31KB	
NTVDM.EXE	C:\WINDOWS\system32	400KB	Microsoft(R) Windows NT(TM) Operating System
nwlghelp.exe	C:\WINDOWS\system32	25KB	Novell Client Login for 32-bit Windows
nwlscript.exe	C:\WINDOWS\system32	18KB	Novell Client for Windows NT
nwsndmsg.exe	C:\WINDOWS\system32	28KB	Novell Client for Windows NT
nwtray.exe	C:\WINDOWS\system32	28KB	Novell Client for Windows NT
odbcad32.exe	C:\WINDOWS\system32	37KB	Microsoft Open Database Connectivity
odbcconf.exe	C:\WINDOWS\system32	76KB	Microsoft Data Access Components
ONDMGNAN.EXE	C:\WINDOWS\system32	10KB	WinINSTALL
OS2SRV.EXE	C:\WINDOWS\system32	128KB	Microsoft(R) Windows NT(TM) Operating System
packager.exe	C:\WINDOWS\system32	73KB	Microsoft(R) Windows NT(TM) Operating System
pax.exe	C:\WINDOWS\system32	53KB	Microsoft(R) Windows NT(TM) Operating System
pbrush.exe	C:\WINDOWS\system32	8KB	Microsoft(R) Windows NT(TM) Operating System
PENTNT.EXE	C:\WINDOWS\system32	67KB	Microsoft(R) Windows NT(TM) Operating System

PERFMON.EXE	C:\WINDOWS\system32	182KB	Microsoft(R) Windows NT(TM) Operating System
PING.EXE	C:\WINDOWS\system32	15KB	Microsoft(R) Windows NT(TM) Operating System
portuas.exe	C:\WINDOWS\system32	34KB	Microsoft(R) Windows NT(TM) Operating System
posix.exe	C:\WINDOWS\system32	67KB	Microsoft(R) Windows NT(TM) Operating System
print.exe	C:\WINDOWS\system32	26KB	Microsoft(R) Windows NT(TM) Operating System
progman.exe	C:\WINDOWS\system32	188KB	Microsoft(R) Windows NT(TM) Operating System
PROQUOTA.EXE	C:\WINDOWS\system32	44KB	Microsoft(R) Windows NT(TM) Operating System
PROSET.EXE	C:\WINDOWS\system32	235KB	Intel PROSet
PSTORES.EXE	C:\WINDOWS\system32	80KB	Microsoft(R) Windows NT(R) Operating System
qbasic.exe	C:\WINDOWS\system32	249KB	
rasadmin.exe	C:\WINDOWS\system32	124KB	Microsoft(R) Windows NT(TM) Operating System
RASMON.EXE	C:\WINDOWS\system32	116KB	Microsoft(R) Windows NT(TM) Operating System
RASPHONE.EXE	C:\WINDOWS\system32	52KB	Microsoft(R) Windows NT(TM) Operating System
RCP.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
RDISK.EXE	C:\WINDOWS\system32	67KB	Microsoft(R) Windows NT(TM) Operating System
RECOVER.EXE	C:\WINDOWS\system32	24KB	Microsoft(R) Windows NT(TM) Operating System
redir.exe	C:\WINDOWS\system32	4KB	
REGEDIT.EXE	C:\WINDOWS\system32	71KB	Microsoft(R) Windows NT(TM) Operating System
regedt32.exe	C:\WINDOWS\system32	194KB	Microsoft(R) Windows NT(TM) Operating System
REGSVR32.EXE	C:\WINDOWS\system32	37KB	Microsoft(R) Windows NT(R) Operating System
			Microsoft(R)

REPLACE.EXE	C:\WINDOWS\system32	29KB	Windows NT(TM) Operating System
restore.exe	C:\WINDOWS\system32	63KB	Microsoft(R) Windows NT(TM) Operating System
REXEC.EXE	C:\WINDOWS\system32	15KB	Microsoft(R) Windows NT(TM) Operating System
ROUTE.EXE	C:\WINDOWS\system32	19KB	Microsoft(R) Windows NT(TM) Operating System
RPCSS.EXE	C:\WINDOWS\system32	103KB	Microsoft(R) Windows NT(TM) Operating System
RSH.EXE	C:\WINDOWS\system32	15KB	Microsoft(R) Windows NT(TM) Operating System
rundll32.exe	C:\WINDOWS\system32	12KB	Microsoft(R) Windows NT(TM) Operating System
runonce.exe	C:\WINDOWS\system32	14KB	Microsoft(R) Windows NT(TM) Operating System
SAVEDUMP.EXE	C:\WINDOWS\system32	23KB	Microsoft(R) Windows NT(TM) Operating System
SC.EXE	C:\WINDOWS\system32	53KB	Microsoft(R) Windows NT(TM) Operating System
secfixup.exe	C:\WINDOWS\system32	41KB	
SERVICES.EXE	C:\WINDOWS\system32	133KB	Microsoft(R) Windows NT(TM) Operating System
setup.exe	C:\WINDOWS\system32	25KB	Microsoft(R) Windows NT(TM) Operating System
setver.exe	C:\WINDOWS\system32	12KB	
share.exe	C:\WINDOWS\system32	1KB	
shmigrate.exe	C:\WINDOWS\system32	43KB	Microsoft(R) Windows NT(TM) Operating System
skeys.exe	C:\WINDOWS\system32	48KB	Microsoft(R) Windows NT(TM) Operating System
slpinfo.exe	C:\WINDOWS\system32	25KB	Novell Client for Windows NT
SMSS.EXE	C:\WINDOWS\system32	40KB	Microsoft(R) Windows NT(TM) Operating System
sndrec32.exe	C:\WINDOWS\system32	113KB	Microsoft(R) Windows NT(TM) Operating System
sndvol32.exe	C:\WINDOWS\system32	62KB	Microsoft(R) Windows NT(TM)

SNMP.EXE	C:\WINDOWS\system32	18KB	Operating System Microsoft(R) Windows NT(TM) Operating System
SNMPTRAP.EXE	C:\WINDOWS\system32	9KB	Microsoft(R) Windows NT(TM) Operating System
sort.exe	C:\WINDOWS\system32	25KB	Microsoft(R) Windows NT(TM) Operating System
spflist.exe	C:\WINDOWS\system32	144KB	SPflist Application
spinit.exe	C:\WINDOWS\system32	20KB	Microsoft(R) Windows NT(TM) Operating System
SPOOLSS.EXE	C:\WINDOWS\system32	35KB	Microsoft(R) Windows NT(TM) Operating System
sprestr.exe	C:\WINDOWS\system32	11KB	Microsoft(R) Windows NT(TM) Operating System
SSWSCHNT.EXE	C:\WINDOWS\system32	72KB	WinINSTALL
subst.exe	C:\WINDOWS\system32	27KB	Microsoft(R) Windows NT(TM) Operating System
sysedit.exe	C:\WINDOWS\system32	19KB	Microsoft® Windows(TM) Operating System
SYSKEY.EXE	C:\WINDOWS\system32	38KB	Microsoft(R) Windows NT(TM) Operating System
systray.exe	C:\WINDOWS\system32	33KB	Microsoft(R) Windows NT(TM) Operating System
TAPISRV.EXE	C:\WINDOWS\system32	150KB	Microsoft(R) Windows NT(TM) Operating System
taskman.exe	C:\WINDOWS\system32	32KB	Microsoft(R) Windows NT(TM) Operating System
TASKMGR.EXE	C:\WINDOWS\system32	84KB	Microsoft(R) Windows NT(TM) Operating System
TCMSETUP.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
TCPSVCS.EXE	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
telnet.exe	C:\WINDOWS\system32	78KB	Microsoft(R) Windows NT(TM) Operating System

TFTP.EXE	C:\WINDOWS\system32	18KB	Microsoft(R) Windows NT(TM) Operating System
TRACERT.EXE	C:\WINDOWS\system32	12KB	Microsoft(R) Windows NT(TM) Operating System
UNLODCTR.EXE	C:\WINDOWS\system32	20KB	Microsoft(R) Windows NT(TM) Operating System
ups.exe	C:\WINDOWS\system32	16KB	Microsoft(R) Windows NT(TM) Operating System
USER.EXE	C:\WINDOWS\system32	47KB	Microsoft® Windows(TM) Operating System
USERINIT.EXE	C:\WINDOWS\system32	27KB	Microsoft(R) Windows NT(TM) Operating System
quikview.exe	C:\WINDOWS\system32\viewers	56KB	Microsoft(R) Windows NT(TM) Operating System
vipx.exe	C:\WINDOWS\system32	2KB	
vlmsup.exe	C:\WINDOWS\system32	16KB	
W00UPD~1.EXE	C:\WINDOWS\system32	368KB	W00Update
winchat.exe	C:\WINDOWS\system32	64KB	Microsoft(R) Windows NT(TM) Operating System
WINDBVER.EXE	C:\WINDOWS\system32	30KB	Microsoft SQL Server
WINDISK.EXE	C:\WINDOWS\system32	173KB	Microsoft(R) Windows NT(TM) Operating System
WINFILE.EXE	C:\WINDOWS\system32	245KB	Microsoft(R) Windows NT(TM) Operating System
winhlp32.exe	C:\WINDOWS\system32	24KB	Microsoft(R) Windows NT(TM) Operating System
WINLOGON.EXE	C:\WINDOWS\system32	184KB	Microsoft(R) Windows NT(TM) Operating System
WINMSD.EXE	C:\WINDOWS\system32	148KB	Microsoft(R) Windows NT(TM) Operating System
winspool.exe	C:\WINDOWS\system32	3KB	Microsoft® Windows(TM) Operating System
winver.exe	C:\WINDOWS\system32	21KB	Microsoft(R) Windows NT(TM) Operating System
wm.exe	C:\WINDOWS\system32	85KB	Novell Client for Windows NT

wmrundll.exe	C:\WINDOWS\system32	6KB	
wmsched.exe	C:\WINDOWS\system32	28KB	Novell Client for Windows NT
wowdeb.exe	C:\WINDOWS\system32	3KB	Microsoft® Windows NT(TM) Operating System
wowexec.exe	C:\WINDOWS\system32	11KB	Microsoft® Windows NT(TM) Operating System
write.exe	C:\WINDOWS\system32	10KB	Microsoft(R) Windows NT(TM) Operating System
XCOPY.EXE	C:\WINDOWS\system32	47KB	Microsoft(R) Windows NT(TM) Operating System
TASKMAN.EXE	C:\WINDOWS	32KB	Microsoft(R) Windows NT(TM) Operating System
TWUNK_16.EXE	C:\WINDOWS	48KB	Twain Thunker
TWUNK_32.EXE	C:\WINDOWS	68KB	Twain Thunker
UNINST.EXE	C:\WINDOWS	293KB	InstallShield unInstaller
unvise32.exe	C:\WINDOWS	84KB	Installer VISE
welcome.exe	C:\WINDOWS	22KB	Microsoft(R) Windows NT(TM) Operating System
WINHELP.EXE	C:\WINDOWS	251KB	Microsoft Windows
WINHLP32.EXE	C:\WINDOWS	304KB	Microsoft Windows

NRC CUSTOM APPL TION SUPPORT LIST

ADD SYS Number	Application Name	System Abbreviation	Sponsor	Type	Support Type	Comments
3603	ACRS Executive Task Management System/Action Item	ACRS-ETMS/AITS	ACRS	Clipper	TS;Install;Config	ASIB NOTIFY
3596	ACRS /ACNW Document Management Systems	ADMS	ACRS	Clipper	Troubleshoot	
2001	Action Item Tracking System	AITS	OE	Clipper	TS;Install;Config	ASIB NOTIFY
3582	Administrative Information Management System	AIMS	NRR	Cobol	Troubleshoot	
3120	Agency Training System	ATS	HR	Cobol	Troubleshoot	
9501	Agencywide Electronic Document Management System	ADAMS	CIO	PeopleSoft	Troubleshoot	
9615	Allegation Management System	AMS	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
3527	Allegation Tracking System	ALTS	OIG	Clipper	Troubleshoot	
9779	Annual Material License Fee	MATANN	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
9660	Applicant Review System (See OP Apps)	ARS	HR	MSAccess	Troubleshoot	
3587	Automated Badge System	ABS	ADM	Clipper	Troubleshoot	ASIB NOTIFY
3573	Automated Performance Appraisal System	APAS	HR	WP Macro	Troubleshoot	
3100	Automated Personnel System	APS	HR	Clipper	Troubleshoot	
3101	Automated Staffing Plan	ASP	HR	Cobol	Troubleshoot	
9671	Branch Action Tracking System	BATS	NMSS	Clipper	Troubleshoot	
3623	Case File Index System	SEC/FOIA	ADM	dBase III+	Troubleshoot	ASIB NOTIFY
3620	Central Office of Record	COR	ADM	Clipper	Troubleshoot	
3014	Central Personnel Clearance Index	CPCI	ADM	Clipper	Troubleshoot	
9896	CISSCO TAC Tracking System	CTACS	CIO	MSAccess	Troubleshoot	
9596	Commission Decision Tracking System	CDTS	SECY	Visual Basic	TS;Install;Config	ASIB NOTIFY
3545	Commission EDO Budget Tracking System	COMEDO	CFO	Clipper	Troubleshoot	
3576	Commision Tracking System	CTS	SECY	Clipper/Macro	TS;Install;Config	
3556	Commision Work Item Tracking System	CWITS	NMSS	Clipper	Troubleshoot	
3531	Commissioner Roger's Mail Tracking System (See OCM)	CMT	OCM	Clipper	Troubleshoot	
3570	Conference Room Schedule System (See ADM Apps)	CRS	ADM	bTrieve/C++	Troubleshoot	

NRC CUSTOM APPLICATION SUPPORT LIST

ADD SYS Number	Application Name	System Abbreviation	Sponsor	Type	Support Type	Comments
9605	Contracts and Payments System	CAPS	ADM	Visual Basic	Troubleshoot	
3300	Criminal History Check System	CHC	ADM	Cobol/DG	Troubleshoot	
3524	Editors' Document Tracking & Database Management Sys	EDITLOG	ADM	Clipper	Troubleshoot	
3528	EDO Document Logging & Location System	DOLLS	EDO	Clipper	TS;Install;Config	ASIB NOTIFY
3554	EDO Foreign Travel System	FTTS	EDO	Clipper	TS;Install;Config	
3621	EDO Label System	EDOLS	EDO	Clipper	TS;Install;Config	
3598	EDO Work Item Tracking System	EDOWITS	EDO	Clipper	Troubleshoot	
9664	Electronic Plant Info Book	EPIP	AEOD	Visual Basic	Troubleshoot	
3514	Employee Drug Testin System	EDTS	ADM	ADSO/Cobol	Troubleshoot	
4000	Employee Exposure Databse	EED	HR	Clipper	Troubleshoot	
2500	Enforcement Action Tracking System	EATS	OE	Power Builder	TS;Install;Config	ASIB NOTIFY
9001	Enhanced Participatory Rulemaking Process	EPRP	RES	BBS Software	Troubleshoot	
1285	Event Notification System (See EN Safety Sys)	EN	NRR	Clipper	TS;Install;Config	
3593	Events Tracking System (See EN Safety Sys)	ETS	NRR	Clipper	TS;Install;Config	
3580	Executive Task Management System	ETMS	ADM	Clipper	TS;Install;Config	ASIB NOTIFY
3632	Facilities Annual Fees (See FEES)	FACANN	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
3507	Facilities Inspection Fees System (See FEES)	FACFEES	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
9604	Federal Register Notices and Comments	FEDREG	ADM	Pascal 7.0	Troubleshoot	
3592	Fees Collect System (See FEES)	COLLECT	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
9778	Fees File Transfer Protocol (See FEES)	FEESFTP	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
9675	FFS Download System	NRDS	NRR	Clipper	Troubleshoot	
9602	FIXIT	FIXIT	ADM	bTrieve/C++	Troubleshoot	
3501	FOIA Actions Tracking System	FACTS	CIO	Clipper	Troubleshoot	
3502	FOIA Office Status System	FOSS	CIO	Clipper	Troubleshoot	
3608	Folder (File Locator System)	FOLDER	ADM	Clipper	Troubleshoot	
3611	FOLIOS Text Management System	FOLIOS	NRR	Views 2.1	TS;Install;Config	
3544	Fuel Cycle System	FUEL	CFO	Clipper	Troubleshoot	

NRC CUSTOM APPLICATION SUPPORT LIST

ADD SYS Number	Application Name	System Abbreviation	Sponsor	Type	Support Type	Comments
3005	Full Time Equivalency	FTE	HR	Cobol	Troubleshoot	
1221	General License Database	GLDB	NMSS	Power Builder	Troubleshoot	
9670	GG Vacancy Announcement System (See OP Sys)	GGVAC	HR	bTrieve/C++	Troubleshoot	ASIB NOTIFY
9766	Guard Productive Hours Tracking System	GUARDTRAK	ADM	bTrieve/C++	Troubleshoot	ASIB NOTIFY
3633	Individual Action Tracking System	IATS	OE	dBase III+	Troubleshoot	
3523	Information Requirements Control Automated System	IRCAS	CIO	Clipper	Troubleshoot	
A0044	Inspection Procedure Authority System (See RPS System)	RPS/IPAS	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
9709	Inspection Procedures (See RPS System)	IP	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
A0045	Inspection Report Tracking System (See RPS Sys)	RPS/IRTS	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
3401	Integrated library System	ILS	CIO	MUMPS	Troubleshoot	
1270	License Fee Billing System	LFBS	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
3585	License Fee Correspondence Tracking System	FEETRAC	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
1289	License Fee Reporting System	FEESFTP	CFO	Clipper	TS;Install;Config	ASIB NOTIFY
1201	Licensing Management System	LMS	NMSS	Clipper	Troubleshoot	
1266	Licensing Tracking System	LTS	NMSS	Clipper	Troubleshoot	
3543	Materials Fee	MATREV	CFO	Clipper	Troubleshoot	
3506	Materials Licenses Fee System	MATSY	CFO	Clipper	Troubleshoot	
9797	New Phonebook System	NRCPHONE	OCIO		Troubleshoot	
3622	NMSS Document Logging & Location System	NMSS-DOLLS	NMSS	Clipper	Troubleshoot	
3607	NMSS Work Item Tracking System	WITS-NMSS	NMSS	Clipper	Troubleshoot	
1400	NRC Personnel Payroll Systems	NRC-PPS	CIO	Power Builder	Troubleshoot	
3539	NRC Personnel Security system	PERSEC	ADM	Clipper	Troubleshoot	ASIB NOTIFY
3526	NRC TLD Direct Radiation Monitoring Network	TLD	RGN-I	Clipper	Troubleshoot	
3609	NRR Work Item Tracking System	WITS-NRR	NRR	Clipper	Troubleshoot	
3320	Nuclear Document System	NMED	CIO	Oracle	Troubleshoot	

NRC CUSTOM APPLICATION SUPPORT LIST

ADD SYS Number	Application Name	System Abbreviation	Sponsor	Type	Support Type	Comments
9506	Nuclear Material Event Database	NUREGS	AEOD	MSAccess	TS;Install;Config	
3525	Nuclear Refulatory Report System	NUREGS	ADM	Clipper	Troubleshoot	
3614	OC Correspondence Tracking System	OCCTS	CFO	Clipper	Troubleshoot	
3625	OCAA What I did All Day	OCCAAWIDAD	OCAA	Clipper	TS;Install;Config	
9403	Office of Personnel Decision Support System	OPDSS	HR	Power Builder	Troubleshoot	
3601	Office of the Controller Salary and Benefits System	OCSB	CFO	Quattro Pro	Troubleshoot	
3597	OGC Work Item Tracking System	OGCWITS	OGC	Clipper	Troubleshoot	
3616	OIG Closed Investigations	OCI	OIG	Clipper	Troubleshoot	
3613	OIG Commission EDO Budget Tracking System	OIGCOMEDO	OIG	Clipper	Troubleshoot	
3548	OIG Resource & Assignment Tracking System	RATS	OIG	Clipper	Troubleshoot	
3540	OIG Travel System	OIGTRAV	OIG	Clipper	Troubleshoot	
9670	OP Vacancy Announcements	OPVA	HR	bTrieve/C++	Troubleshoot	
1236	Operator License Tracking System	OLTS	NRR	Cobol	Troubleshoot	
3590	Paper Tracking System	PTS	OCAA		Troubleshoot	
1400	Pay/Pers	Pay/Pers	CFO	ADA Base/Natural	Troubleshoot	
3003	Payroll	PAY	CFO	Cobol/IDEA/CQCA	Troubleshoot	
3594	PC/LAN Integrated Events	PIE	NRR	Clipper	Troubleshoot	
9626	PC-Based RITSCard	PC-RITSCARD	NMSS	Power Builder	Troubleshoot	
9596	Personal Librarian Software	PLS	CIO	CDTS	Troubleshoot	
3539	Preprocessing Module	PERSEC	ADM	Clipper	Troubleshoot	ASIB NOTIFY
3628	Printing, Publications, Distribution Tracking System	PPDTS	ADM	Clipper	Troubleshoot	
3548	Processing Module	PROC	ADM	Clipper	Troubleshoot	
9699	Public Affairs Resources System	PARS	OPA	WP/Pers Librarian	Troubleshoot	
3569	Public Meeting Notice System	PMNS	ADM	Clipper	Troubleshoot	
9515	Publications Printing Process	P3	ADM	Pascal 7.0	Troubleshoot	
3508	Reactor Fee System	REACTRA	CFO	Clipper	Troubleshoot	
9709	Reactor Program System (RPS)	RPS	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
3615	Reciprocity Tracking System	RTS	NMSS	Clipper	Troubleshoot	

NRC CUSTOM APPLICATION SUPPORT LIST

ADD SYS Number	Application Name	System Abbreviation	Sponsor	Type	Support Type	Comments
H0039	Record Classification Actions System	RCA	ADM	Clipper	Troubleshoot	
2001	Region II Action Item Tracking System	AITS-RII	RGN-II	Clipper	Troubleshoot	
1295	Regulatory Information Tracking System - AEOD	RITS-AEOD	AEOD	Power Builder	Troubleshoot	
9679	Regulatory Information Tracking System - NMSS	RITS-NMSS	NMSS	Power Builder	Troubleshoot	
1279	Regulatory Information Tracking System - Refions	RITS-NRR	NRR	Power Builder	Troubleshoot	
3550	Reinvestigation System	REINV	ADM	Clipper	Troubleshoot	
3599	research Information Management System	RIMS	RES	Paradox	TS;Install;Config	ASIB NOTIFY
9696	Roster of Utilities (On the web)	RUTIL	NRR	WP Macro	Troubleshoot	
3538	Safeguards Events Analysis	SEA	NMSS	Clipper	Troubleshoot	
1216	Safety Issues Management System	SIMS	NRR	Cobol	Troubleshoot	
1212	Sealed Source & Device	SSDS	NMSS	Clipper	Troubleshoot	
3589	SECY BBS	SECY	SECY	BBS Software	Troubleshoot	
9509	Secy Tracking and Reporting System	STARS	OCM	Client Server	TS;Install;Config	ASIB NOTIFY
9595	Site Decommissioning Management Plan	SDMP	NMSS	C++	Troubleshoot	
A0046	Systematic Assessment of Licensee Performance	RPS/SALP	NRR	Power Builder	TS;Install;Config	ASIB NOTIFY
1208	Technical Assignment Control System	TACS	NRR	Power Builder	Troubleshoot	
1225	Time Sharing Accounts Management System	TAMS	CIO	Cobol	Troubleshoot	
9794	TQMB Task Management System	TTMS	NRR		Troubleshoot	
1265	Transport Approval Package Information System	TAPIS	NMSS	Clipper	Troubleshoot	
9670	Vacancy Announcement Tracking	VAT	HR	bTrieve/C++	Troubleshoot	
H0040	Visitor Information Profile	VIP	ADM	bTrieve/C++	Troubleshoot	
9006	Westinghouse AP600/GE SBW	AP600	NRR		Troubleshoot	
9718	What I Did All Day for Windows	WINWIDAD	OGC	Delphi	Troubleshoot	
1234	Work Item Tracking System	WITS	AEOD	Clipper	Troubleshoot	

User Support Services

Metric/Measurement	Measure
CALLS	
Number of Calls	daily/weekly/monthly/ yearly reports
Number of Calls per hour	peak/non-peak intervals
Number of calls or email requests during off-hours	daily, weekly, monthly
Average answer time per calls	peak/non-peak intervals
Calls answered and abandoned	peak/non-peak intervals
HELP DESK	
Number of Tickets Opened	daily, weekly, monthly, quarterly
Percentage of tickets resolved on first contact	peak/non-peak intervals monthly/quarterly
Top 10 Tickets by Category Type	daily, weekly, monthly, quarterly
Distribution of Tickets by Office	monthly
Satisfaction Surveys	monthly/quarterly reports
ACCOUNTS	
Number of user accounts on network (# of seats)	weekly, monthly
Number of accounts added, deleted	daily, weekly, monthly
Amount of network space available to each user	daily

Non-Network Components

Metric/Measurement	Measure
COMPONENTS	
Inventory by device (pc, scanner, laptops, etc	monthly
Number of Hardware Installs	weekly/monthly/yearly reports
Number of Maintenance tickets	weekly/monthly/yearly reports
Problem rate by device	average downtime per type unit / MTBF* (annual report)
Hardware failures within a time period	weekly, monthly
Response time to repair	
Number of repeat calls from user for same problem	Daily, weekly, monthly
Loaner equipment (laptop computers, PDAs, etc.)	semi-annual reports

* MTBF = mean time between failure

Network - Components/Connectivity/Performance/Productivity

Metrics	Measure
AVAILABILITY	
Network Availability	Monitor up/down status of network to ensure that it's available and accessible (up/down connectivity-HQ & regions).
Remote Access Availability (devices)	Monitor the availability of all remote access devices and lines to maintain reliable remote access to the network. Poll every minute.
File, Print and Application Server Availability	Monitor all LAN servers to ensure they are available and accessible (% up time). Poll every minute.
Server Disk Availability	Monitor disk availability on all LAN servers to ensure disk space is not exhausted. Poll every minute.
LAN Hardware	Monitor all LAN hubs and switches to ensure they are available and accessible. Poll every minute.
LAN Segments	Monitor all LAN segments to ensure they are available and accessible. Poll every minute.
Electronic Performance Monitoring, Incident Detection and Diagnostic Service	
Network Utilization	Monitor network utilization to maintain reliable performance.
WAN Link Utilization	
Network Performance	Identify/monitor average and peak utilization of network bandwidth, network servers, and high performance systems.
Network throughput	Usage rate: % bandwidth used at a given time
Remote Access Capacity	Monitor the usage on each of the remote access devices to maintain reliable remote access to LAN devices. Poll every minute.
Server Performance	Monitor all LAN servers to ensure high performance, including time between receiving requests to responding with data.

Metrics	Measure
Router performance	<p>Monitor if router is overloaded and starting to drop packets. Track router CPU utilization and dropped packets (graphs depicting daily statistics)</p> <p>Average and peak utilization of individual router interfaces and percentage of errors (high utilization and high error rates result in poor network performance).</p>
Gather RMON statistics from hubs and switches	Run an RMON report to show if utilization is high.
Response Time	<p>Server Performance: time between receiving request to responding with data.</p> <p>Network performance: total transaction network time.</p> <p>Round-trip performance: end-to-end delay for a single packet.</p> <p>Transaction response time: end-to-end response time from end of submit at user's PC to a fresh PC screen.</p>
CPU Utilization On All Servers	Monitor the CPU utilization on all LAN servers to maintain reliable performance
Ethernet LAN Segments	<p>Monitor the utilization on each Ethernet LAN segment to maintain reliable access to LAN devices.</p> <p>Poll every minute.</p>
Server Virtual Memory Utilization	<p>Monitor the virtual memory utilization on all LAN servers to maintain reliable performance.</p> <p>Poll every minute.</p>
Server Physical Memory Utilization	Monitor the physical memory utilization on all LAN servers to maintain reliable performance
Network Bandwidth	Bandwidth per user, application and service
Network Data Loss	Loss rate
Ethernet Error Rates	Monitor the error rates on each Ethernet LAN segment to maintain reliable access to LAN devices
Ethernet Collision Rates	Monitor the collision rates on each Ethernet LAN segment to maintain reliable access to LAN devices.
Network Traffic Patterns	

Metrics	Measure
Identification of Bottlenecks	
Electronic Notification Service	Components which are powered up, operating, and network connected.
Alarming	Percentage of time an event occurs and successful notification is received within a specific time period.
Electronic Software Distribution	Components which are powered up, operating, and network connected.
Software Maintenance on network	% upgrades executed on schedule. % upgrades successfully completed within a specific time period.
Software Management – Version Control	
Electronic Topology/Configuration Management	Configuration Management for all DCE components: Current description of image, current configuration of hardware and software, current location . Accessible by NRC.
Performance Analysis and Tuning	Components which are powered up, operating, and network connected.
Network Performance Trending	
Baseline for Network Performance	
Network File Backup	
Local Drive Storage Backup to Network	Data files in Standardized Directory only for components that are powered up, operating, and connected to the network.
Shared Network Storage Data File Backup	
Disaster Recovery Shared Network Storage Data File Backup	
Backup Media Rotation and Media Retention	Percentage of tasks completed on schedule
Server Back and Restoration	Percentage of time hosting vendor can complete the task within a predetermined time period
Response to Complete File Restores	Percentage of time hosting vendor can complete the task within a predetermined time period
Growth management projections for media backup	Measure storage, usage by user and servers
OTHER	
External Web access to firewall and through firewall	

Metrics	Measure
Network Security	Encryption Key Management Effect on performance
Network Service and Support	Support contacts Response time Network outages Service upgrades and revisions
Baseline for Network Performance	
SERVICE LEVELS	
User Account Management (create, modify, delete user accounts - access privileges)	Percent of requests completed within a specific time.
Electronic Messaging Services Management (create, modify, delete user mailbox)	Percentage of requests that are completed within a defined time period.
Printer Management/ Administration	Percentage of requests that are completed within a defined time period.
Mean Time to Service Provisioning	Time from receiving order and availability of service.
Mean Time to Service Restoration	Time from receiving trouble ticket until return of service.

Software/Applications

Metrics	Measure
Time-Frame for Application Availability	
Throughput (e.g., end-to-end measure of e-mail messages)	Average peak throughput in transactions, packets, or Kb per second
Per-site Application Availability	<p>Ratio of time application is available to total time per month warranted time.</p> <p>Total cumulative uptime or downtime in the monthly interval of warranted application availability.</p>
Security	Control or limitations such as password protected, virus scanning, etc.
Response Time	<p>Server Performance: time between receiving request to responding with data.</p> <p>Network performance: total transaction network time.</p> <p>Round-trip performance: end-to-end delay for a single packet.</p> <p>Transaction response time: end-to-end response time from end of submit at user's PC to a fresh PC screen.</p>
CITRIX (Remote Access)	# of users
Remote access usage	
Disk Space Used by Mail System	
Number of ADAMS calls to Help Desk	semi-annual reports
Number of STARFIRE calls to Help Desk	semi-annual reports
Number of Software Packages installed	weekly/monthly/yearly reports

NRC REMOTE STATUS WEEKLY UPDATE
 May 23, 2001

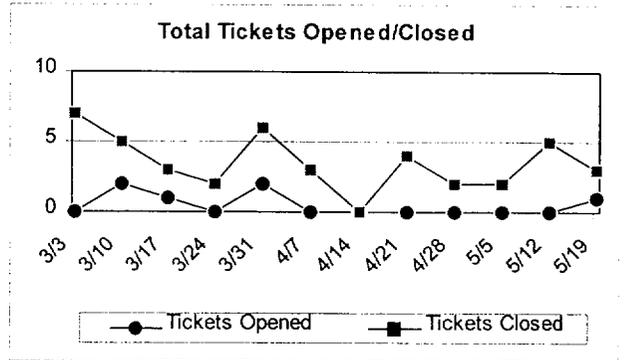
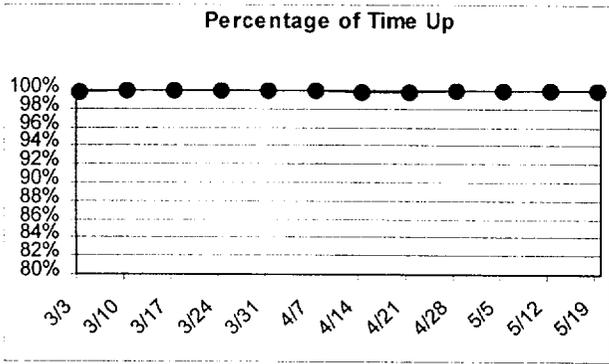
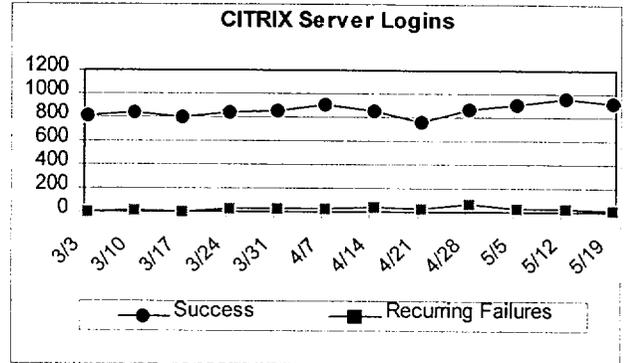
A. New Initiatives - New user friendly front-end (CITRIX Client version 3.0) - 622 copies distributed as of 5/18/01.

ISSUES 1. Some "home use" printers are not NT compatible.

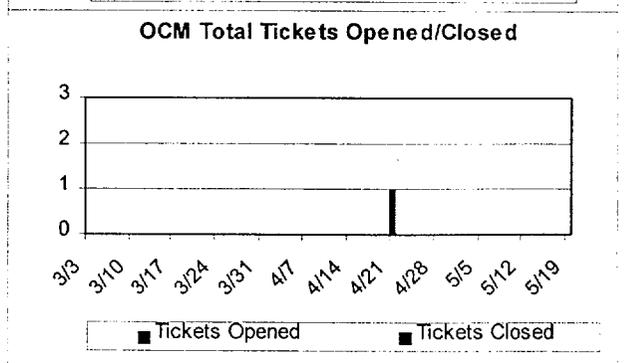
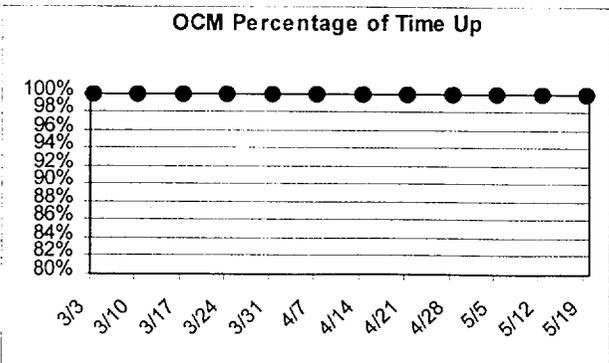
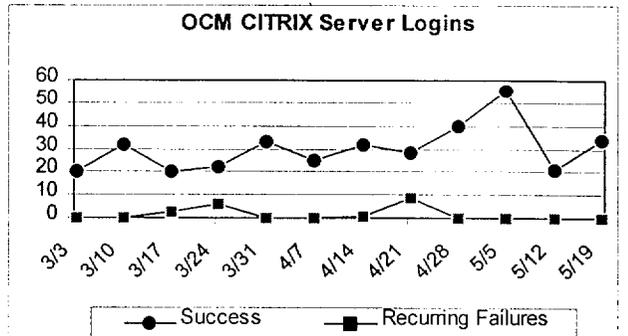
B. Production Services - Remote Access Accounts - 2030 Agency-wide.
 Number who have used the HQ general use server successfully to date - 1166 of 1166 accounts.

Regional Accounts Created			
Region I	230	Region III	198
Region II	245	Region IV	191

NOTE: Recurring Failures - users not successfully logging in after several attempts 1.66%.



C. Senior Management - Remote Access Accounts - 65 - used successfully to date - 50.



Handwritten text inside a rectangular box, possibly a signature or a name.

Release Management Process Overview

Table of Contents

1.0	Background	1
2.0	Purpose	1
3.0	Approach	1
4.0	Overview of Release Management	1
5.0	Release Management	2
5.1	Release Management Phases	2
5.1.1	New Revision Requirement Analysis	2
5.1.2	Release Identification Phase	4
5.1.3	Combined Testing Phase	4
5.1.4	Release Management (Provisioning) Phase	4
5.1.5	Release Phase	5
5.2	Release Management Interfaces, Inputs and Outputs	5
	Attachment A - Sample Schedule	7

List of Figures

Figure 1	3
----------------	---

1.0 Background

Sytel, Inc. of Bethesda, MD is the successful offeror on the U.S. Nuclear Regulatory Commission's (NRC), "Next Generation Network" contract. With its subcontractor, CEEXEC, Inc., Sytel will be supporting the NRC's existing Agency Wide Network (AWN), while designing, developing, and installing the Agency's Next Generation Network (NGN).

2.0 Purpose

Release Management (RM) provides a process by which changes made to the Production Operations Environment (POE) can be made effectively and efficiently. The process enhances the effectiveness of the Infrastructure Development Process Model (IDPM) by providing the specific mechanism by which the properly developed, tested and integrated new technologies, developed in accordance with the IDPM, can be most efficiently implemented within their full scope. Release Management has the greatest impact upon Agency-wide software components of the NRC's network and is very tightly coupled to Configuration Management (CM). RM is an iterative process that has two entry points and exit points on the linear IDPM. This coupling ties the Operations and Support Phase of the IDPM back to the Transition and Implementation Phases of the IDPM enhancing the support phase by providing a mechanism that enables a continuous improvement process for POE components. RM also provides a mechanism for new technology just developed in the IDPM to be released into the POE in a controlled and well thought out manner.

3.0 Approach

The intent of the IDPM is to provide not only a methodology to develop new technology, but to form a framework for all other POE and development processes to plug into. RM is a process that plugs into the IDPM framework, an enhancement to be used with the IDPM, not a tool to skip IDPM steps or a work around to the IDPM. This document defines the process of RM, but also provides specific entry points and exit points on the IDPM, the interfaces, and inputs and outputs expected from the processes involved. RM, in the form as presented here, is not meant to be a complete stand alone process and therefore does not include many elements that a stand alone process would contain. The main goal in this approach is to avoid developing any excessive processes and to keep the amount of documentation and the complexity to a minimum.

4.0 Overview of Release Management

Release Management will coordinate the release of, primarily, new software components and fixes into the POE. It will provide for the development of the policies, procedures, roles, and responsibilities required to control this release. As with the IDPM, RM will be described as a series of process steps or phases. The requirement for a release is always generated in an IDPM phase and enters the RM process at that point. RM will then review the requirement and it will pass that requirement to the group responsible for revising the product or to Release Management depending on the nature of the product to be released. There will then be a combined testing, integration and acceptance phase. New technology passing directly to Release Management will be the initial release of a new technology and will not pass through the combined testing phase as that aspect will have been covered by previous IDPM steps. Release Management will determine the form of release, either stand alone or image based,

depending on the business needs of the NRC and the needs of the network. Nothing will be processed for release without going through the Release Management group, a subset of the POE Provisioning group (Tier 3). The Configuration Manager is the single point through which anything and everything must pass before it is released on the NRC network.

5.0 Release Management

The Release Management Process will be described in two parts. The first will be a detailed description of each RM step or phase. Following that will be a description of the interfaces of RM to other processes and finally, the inputs and outputs expected at those interfaces. There is also a process flow drawing (please see Figure 1 on the next page) to provide a quick reference to the RM process and its relationship to other POE processes and the IDPM and Configuration Management.

Candidates for release into the POE, or Release Candidates (RCs), can follow a number of finite paths through the Release Management Process (RMP) as several phases have two distinct, separate, mutually exclusive sub-processes. Each of these sub-processes will be detailed in the appropriate order. The exact process an RC will take will depend on the nature of the RC. It can be anything from a minor bug fix to a completely new unreleased Agency-wide application.

As the name implies, Release Candidates are just that, candidates for release. Having designed some new technology, performed a bug fix or upgraded an existing system does not qualify anything for release into the POE without the proper controls and processes in place. Although highly unlikely, an RC could be blocked at this stage from release depending on the findings of the Release Manager. The Release Manager is the final safety checkpoint before anything can be released into the POE and therefore, since the responsibility of the POE's safety is in his hands, so must the authority to stop an RC from being deployed if there is reason to believe that the stability, supportability or reliability of the POE is at risk.

The possible tracks that an RC can follow will result in the RC becoming a stand alone release or an image release. A stand alone release will be a deployment of the RC as an implementation package unto itself. The image release will be a deployment of the RC along with other RCs incorporated into the standard workstation or server image. Eventually, even a standalone release will be integrated into the image, the stand alone release will have some quality that warrants releasing it on an individual basis rather than with other RCs.

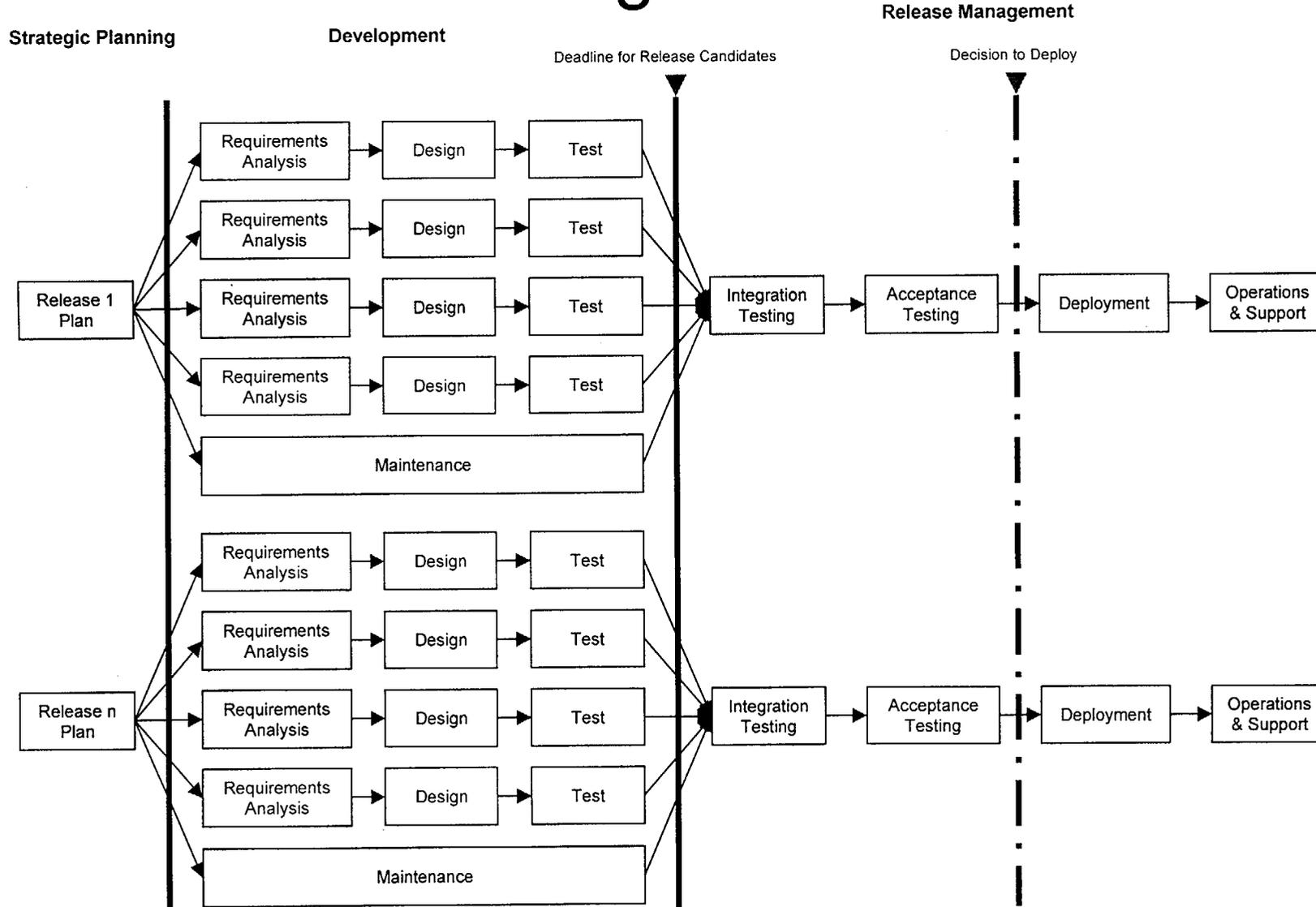
5.1 Release Management Phases

5.1.1 New Revision Requirement Analysis

Whenever a new requirement for new functionality, a correction to a deficiency, a change to a server component, such as a database, etc. arises, the first step will be to analyze the requirement. In the case of a deficiency or bug, the bug must be documented completely and testing must be done to determine the extent of the deficiency. The requirement could also be part of a contractual agreement between the NRC and a developer to deliver subsequent versions of a package developed for the NRC POE. Regardless of the origin or initiation of this phase, the documentation should be complete so that it is understood by all stakeholders,

exactly what is included in the new release. This phase is initiated from outside of release management and is the phase that defines the basic contents of most Release Candidates.

Release Management Overview



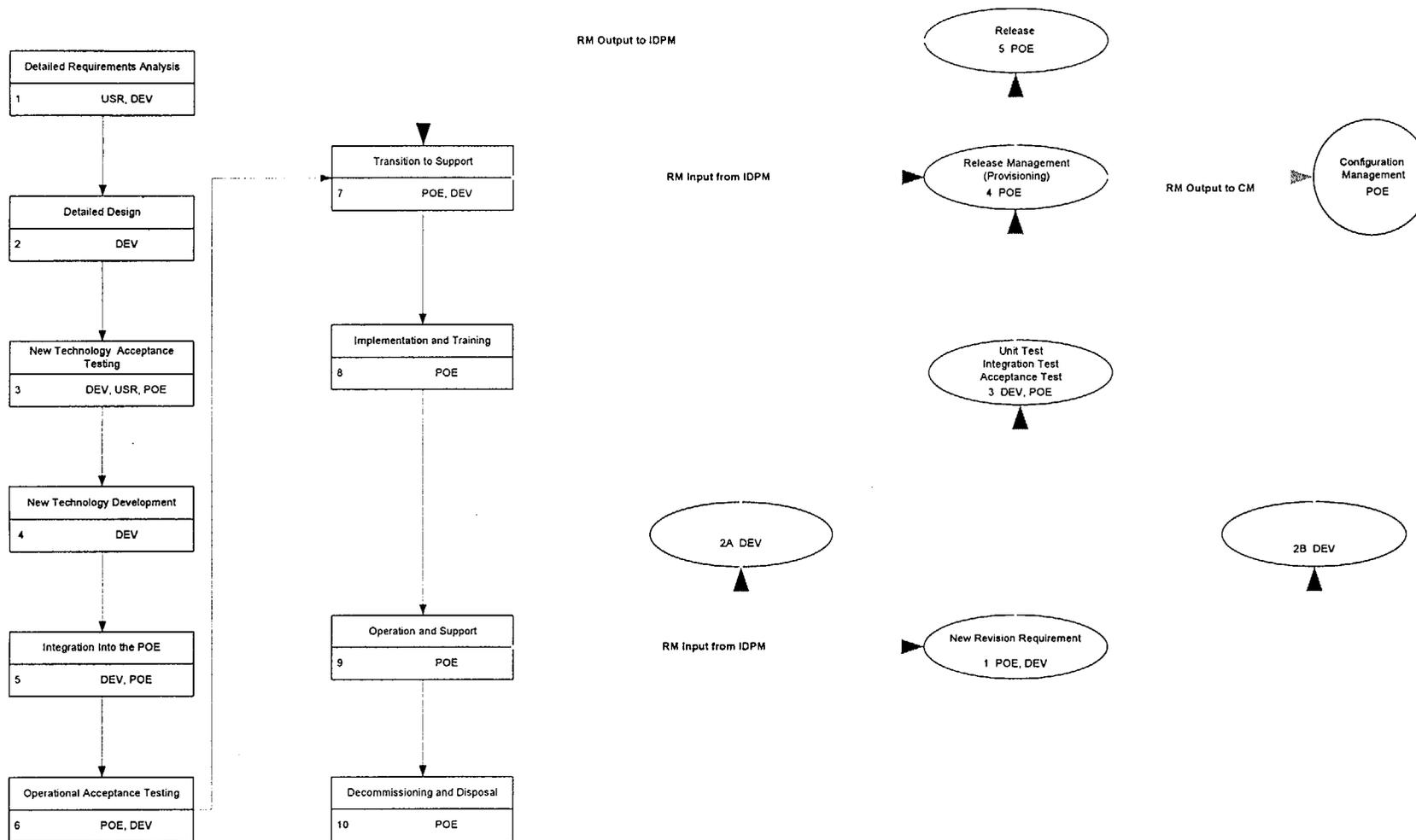


Figure 1

5.1.2 Release Identification Phase

This phase consists of two mutually exclusive sub-processes, categorized as significant or ancillary. The two processes are defined by the level of complexity, and the amount of documentation necessary for the provisioning of the candidate. A major distinction between the two is the nature of the work involved by the developer. The distinction is made to explicitly assert the responsibilities of the developers and the deliverables required with the RC to proceed to the Release Management (Provisioning) Phase.

- A. The ancillary process phase - This is the simple case of an RC that can be deployed into the POE or a part of the POE that does not require any new or changed documentation. It will not require any training for users or that any other major work be performed. The simplest example of an RC that fits this category is a bug fix to repair a minor deficiency in a part of the POE that slipped past the rigors of the IDPM. The deliverables that the developer is to provide with this RC will include a complete description of the reason this RC has been developed and a complete description of what it does and how it is to be integrated. For the example of the bug fix, this would be the complete bug description, the complete documentation on what parts of the bug are corrected and the preferred method for integrating or applying the patch.
- B. The significant process phase - This case is the complex case of the second Phase. The development of this RC will require the re-release of documentation, major user interface changes, changes to a server image (server image changes are never considered trivial and therefore will always be considered in this sub-process only), re-training of users, or a major disruption of POE services. The deliverables required for an RC that fits into this classification are more extensive and require more effort to complete. The testing of the RC will also be more in depth and require more resources. The POE provisioning group will be more involved in the testing and acceptance process than with the previous case. An example of this case would be a minor revision of deployed software to add functionality or to correct major deficiencies that slipped by the IDPM processes. It is important to note that a major revision or a new module to be added to an existing POE system should follow the appropriate IDPM stages before reaching an RM interface.

5.1.3 Combined Testing Phase

This phase is a combination of all of the testing done in the IDPM. In either of the previous cases, the changes are not extensive enough to warrant the full IDPM process of testing, integration and testing. A test plan must still be written by the developer and approved by at least the release manager or the POE Provisioning group. The tests should be performed and data recorded as in the IDPM testing processes and all stakeholders should be notified and attend the testing where applicable or desired. The POE Provisioning Group will be in attendance during any acceptance testing and must be satisfied, as in the IDPM, that the RC has passed all tests, performs as it is intended, and poses no threats to the POE. Copies of all test data will accompany the RC to the Release Manager to be placed in the OPs groups records.

5.1.4 Release Management (Provisioning) Phase

This is the main phase of the Release Management process and requires a high level of coordination. It is therefore necessary that this phase be actively monitored and guided by a dedicated resource. This resource is the Release Manager. The Release Manager is the focal point of each release cycle whether it is an image type or a stand-alone type of release. The responsibility of the Release Manager is to ensure that all RCs that are received are accompanied by the required documentation and that the RC will not cause any harm or disruption to the POE. The Release Manager has the final authority over the RC and its final disposition. Each release cycle will have an associated Release Manager assigned to it. The release cycle itself will be divided into sub-processes as follows:

1. Collection
2. Integration
3. Testing
4. Approval

The collection process will be the time in which a developer can submit an RC for release during that cycle. After this period, the RC may not be accepted for incorporation into the release, even if the RC has been scheduled for release in that cycle. The integrity of the POE and all of its associated applications, services and functionality, must be considered above any single application. By not setting strict deadlines and requirements for submission, the integrity of the POE is put at risk. The integration of the various RCs into an image based package follows the collection process. This process will be considerably easier in the case of a stand-alone release. It is important to note that this is strictly the integration of the release package. Any integration work for the RC to function correctly in the POE should have been performed, tested and proven long before this process. Following the integration process is the testing process. Again, this is a test of the release to the target workstations or servers, not a test of any specific RC. The approval stage is the final authorization by the NRC Operations management to proceed with release. This phase and its sub-processes are shown in the sample schedule in Attachment A.

5.1.5 Release Phase

Release is the final phase of RM. It is simply the release of the software into the POE. The Release Manager monitors the release to ensure that it is executed without incident. The Release Manager should coordinate any responses required in the event of a failure of the release package. Otherwise, the details of the release are left to the IDPM and its appropriate phases and processes.

5.2 Release Management Interfaces, Inputs and Outputs

The interfaces to Release Management are confined to two phases of the IDPM: the Transition to Support Phase and the Operations and Support Phase. In most cases, the main interface for output from the IDPM to the RM process will be from the Operations and Support Phase. The only output from the IDPM that will not come from this phase of the IDPM will be the case of a brand new release of new technology, a new module for an existing POE system, or a major revision to a POE system. To put it in other words, any process that was initiated in and

followed the IDPM will fall into this latter category while RCs generated due to operational or contractual issues will be the former case.

1. **Input: IDPM Operations and Support Phase to RM New Release Requirement Phase**

During the course of a system's life cycle, if it is found to have some deficiency, lack of functionality, unanticipated effect, or similar problem, the problem will be reported to the proper group by the Operations group. The problem will be completely documented with all known information and the results of the tests done to confirm the problem as well as any subsequent testing or findings. An appropriate tracking number should be assigned so that the problem can be documented and tracked properly.

2. **Input: IDPM Transition to Support Phase to RM Release Management (Provisioning) Phase**

As new technology proceeds through the IDPM, there will come a point where deployment of the new technology is required. To properly manage the deployment and create a deployment package, the new technology will be released into the Release Management (Provisioning) phase of the RM process. This will give the Release Manager the time to review all of the requirements for the release and make the final release decision before the new technology moves into the IDPM Implementation and Training Phase.

3. **Output: RM Release Management (Provisioning) Phase to Configuration Management**

Once the new technology becomes an approved release candidate and the release manager has certified it for release into the POE, the appropriate Configuration Management Process must be started to document the changes to the POE to reflect the addition of the new technology. The entry point into Configuration Management will be through the Change Management Process.

4. **Output: RM Release Phase to IDPM Transition to Support Phase**

This is essentially the release of the new technology back to the IDPM for deployment. The RC and all of the required deliverables will have been checked and found appropriate for release into the POE. The release methodology has been determined, deployment is scheduled, and all required approvals have been obtained.

Attachment A - Sample Schedule

**Release Management
Procedures**

Draft

November 8, 1999

Table of Contents

1	Define Release Life Cycle Dates	1
2	Identify Release Candidates (RC)	1
3	Update/Upgrade, or Maintenance RC Requirements Review	2
4	IDPM Requirements Analysis Review	2
5	Assign Target Release Date	2
6	IDPM Design Phase	2
7	IDPM Test Phases	2
8	RC Documentation Submitted to CM	3
9	CM Documentation Review and Acceptance	3
10	Release Assignment	3
11	RM Acceptance of Release Candidates	3
12	Standalone Release	3
13	RC Integration into Release Package	4
14	Release Package Testing	4
15	Release Package Pilot Testing	4
16	Rejected Package Review	4
17	Release Package Transition to Support	4

List of Figures

Figure 1	Release Candidate Procedures	7
----------	--	---

Procedural steps are numbered to match Figure 1, found on page 7.

1 Define Release Life Cycle Dates

Deadlines must be defined to implement the management of release candidates (RC) into the POE. The strategic planner, configuration manager (CM), and release manager (RM) define and publicize the following dates:

Step	Deadline	Definition
2	Initial RC notification	Final day the CM may be notified of an RC item for potential assignment to a release.
5	RC target date assignment	Last day an RC may be assigned a target release date for the package.
8	RC documentation submittal - <i>IDPM candidates only</i>	Last day completed RC IDPM documentation may be submitted to CM.
11	RC acceptance date	Final date RC may be accepted by RM, last day control of RC may pass from CM to RM. All documentation has been reviewed and accepted by CM.
13	Completion date for integration into the release package	Date RC must pass integration testing.
14	Release package testing	Date release package must pass individual package testing.
15	Release package pilot testing	Date package must pass pilot testing and release to IDPM phase 7, transition to support.
17	Release package transition to support	Date package is sent to IDPM phase 7, transition to support.

These dates are to be publicized along with points of contact for each deadline. The CM carries prime responsibility for the coordination and timing of the releases as a group. Should a release package become delayed, the CM will determine whether or not to continue with the delay or to integrate the entire release into the next cycle.

2 Identify Release Candidates (RC)

Once a Release Candidate has been identified, written notification (e-mail or paper copy) must be sent to the CM no later than the due date for this task. Notification will consist of a brief statement of work, and will include a high-level description of what the RC is, the purpose, an estimation of work effort, priority ranking, and the source point of contact of the RC.

The CM assigns a release candidate number to each RC. Coding of the RC will be a concatenation of the release designation, year, candidate type, and the iteration. This number will be assigned based on the year the candidate is identified, and is not changed through the life cycle of the candidate. The CM is responsible for tracking the submissions and assigned

candidate numbers. A log will be maintained and made available to any member of the contract or the NRC.

<i>Release Designation</i>	<i>Year</i>	<i>Candidate Type</i>	<i>Iteration</i>	<i>Sample Release Candidate Assignments</i>
<i>RC</i>	<i>00, 01, etc.</i>	<i>W (workstation)</i>	<i>001, 002, +1</i>	<i>RC00W001</i>
<i>RC</i>	<i>00, 01, etc.</i>	<i>S (server)</i>	<i>same</i>	<i>RC01S213</i>
<i>RC</i>	<i>00, 01, etc.</i>	<i>I (infrastructure)</i>	<i>same</i>	<i>RC01I050</i>

3 Update/Upgrade, or Maintenance RC Requirements Review

RCs in this category may not require significant documentation. The CM is responsible for defining the documentation needs. Each RC will require varying levels of detail; for example, a bug would need only the bug report. Review of the documentation is done by the CM. Step 4 is skipped, continue to Step 5.

4 IDPM Requirements Analysis Review

Completed analysis of an RC from the IDPM life cycle is submitted to the CM for review. The CM is responsible for conducting any review meetings he/she feels are necessary before moving to the next procedure, assigning a targeted release date. If the analysis is not complete, the CM can reject the release candidate, returning the candidate back to the analysis phase of the IDPM.

5 Assign Target Release Date

The CM assigns a targeted release date to the RC. Coding of the targeted release date will be a concatenation of the release type, year, and release number within the year. The CM is responsible for tracking the submissions and assigned target dates so that they are available to any member of the contract or the NRC.

<i>Release Type</i>	<i>Year</i>	<i>Release Number</i>	<i>Expected Frequency</i>	<i>Sample Release Number Assignments</i>
<i>W (workstation)</i>	<i>00, 01, etc.</i>	<i>Q1, Q2, Q3, Q4 or SA01, SA02, SA03, etc.</i>	<i>Q - quarterly SA - stand alone, incremented +1</i>	<i>W00Q1, W00SA01</i>
<i>S (server)</i>	<i>00, 01, etc.</i>	<i>V1, V2, etc.</i>	<i>as needed, expected semi-annually</i>	<i>S00V1, S00V2</i>
<i>I (infrastructure)</i>	<i>00, 01, etc.</i>	<i>V1, V2, etc.</i>	<i>as needed, expected annually</i>	<i>I00V1, I00V2</i>

6 IDPM Design Phase

Refer to the IDPM. All documentation is to be included in step 8.

7 IDPM Test Phases

Refer to the IDPM. All documentation is to be included in step 8.

Begin Release Acceptance Phase

8 RC Documentation Submitted to CM

All documentation through Phase 7 of the IDPM; to include analysis, design, test plans, and test results, are submitted to the CM by the deadline defined in step 2. Missing or incomplete documentation may be returned to development for completion before the CM accepts the RC as a candidate for integration into its scheduled release.

9 CM Documentation Review and Acceptance

The CM documentation review is an assurance check done to prevent introducing items into the production operation environment that do not meet the standards necessary to assure a smooth transition into the release phase. The CM will review all documentation and conduct any review meetings he/she feels are necessary. The CM will make the final decision whether to release the RC into the targeted release, or to reassign it to a subsequent release. Should the documentation review result in a rejected RC, the CM will return the RC to development for revision. Only the CM may change the release assignment. The CM is responsible for maintaining logs for each RC to include review dates, status, issues, and release assignment number.

10 Release Assignment

The CM assigns the RC a release number, determining if the targeted release date can be met. Control of the RC and all documentation is passed to the Release Manager (RM) of the assigned release.

Begin Provisioning Phase

NOTE: *At the completion of each testing phase, the RM must review and pass each test iteration before it may continue to the next step. The RM can, at any point in the provisioning phase, reject a candidate and return it to the IDPM development cycle. IDPM support staff participate in this phase.*

11 RM Acceptance of Release Candidates

Release candidates must be accepted by the RM no later than the deadline defined in step 2 to be included in a release package. The RM reviews all documentation and assigns test plan writing and execution to staff members. Test plans and their results are to be written, reviewed, and accepted at all three stages of testing: package integration, package testing, and pilot testing. The RM is responsible for management and control of the release package through the provisioning phase.

12 Standalone Release

Standalone releases will be required when there is a need to implement the release as soon as possible. A standalone package does not require integration release package testing (step 13), but must go through release package testing and pilot testing.

13 RC Integration into Release Package

Each RC will be integrated into the release package and tested to assure the compatibility between RC items. Integration of each RC into the release package requires a written test plan. Test plan and results are reviewed by the RM. The RM tracks the status of each RC as integration is completed. Control of any RC that fails the package integration is returned to the CM, and the RC is removed from the package. Passing this phase is a requirement before the package moves to package testing in step 14.

14 Release Package Testing

The final package is tested on clean workstations of varying varieties. Test plan and results are required. The RM reviews the test results before passing the package on to pilot testing, step 15. If the package fails, the CM is given control of the package.

15 Release Package Pilot Testing

The package is pilot tested on current user workstations. Test plans and results are reviewed by the CM, with the go/no go decision made by the CM to pass the package on to the transition to support phase of the IDPM.

16 Rejected Package Review

The CM reviews and may redefine the requirements of a package that fails the pilot test. Control of the package and these requirements are then returned to IDPM development. The RCs of the package are then re-evaluated and assigned a new release date.

17 Release Package Transition to Support

Control of packages that have passed the pilot testing is passed to Phase 7 of the IDPM, Transition to Support.

Action Plan Checklist

RM Release Manager

RC Release Candidate

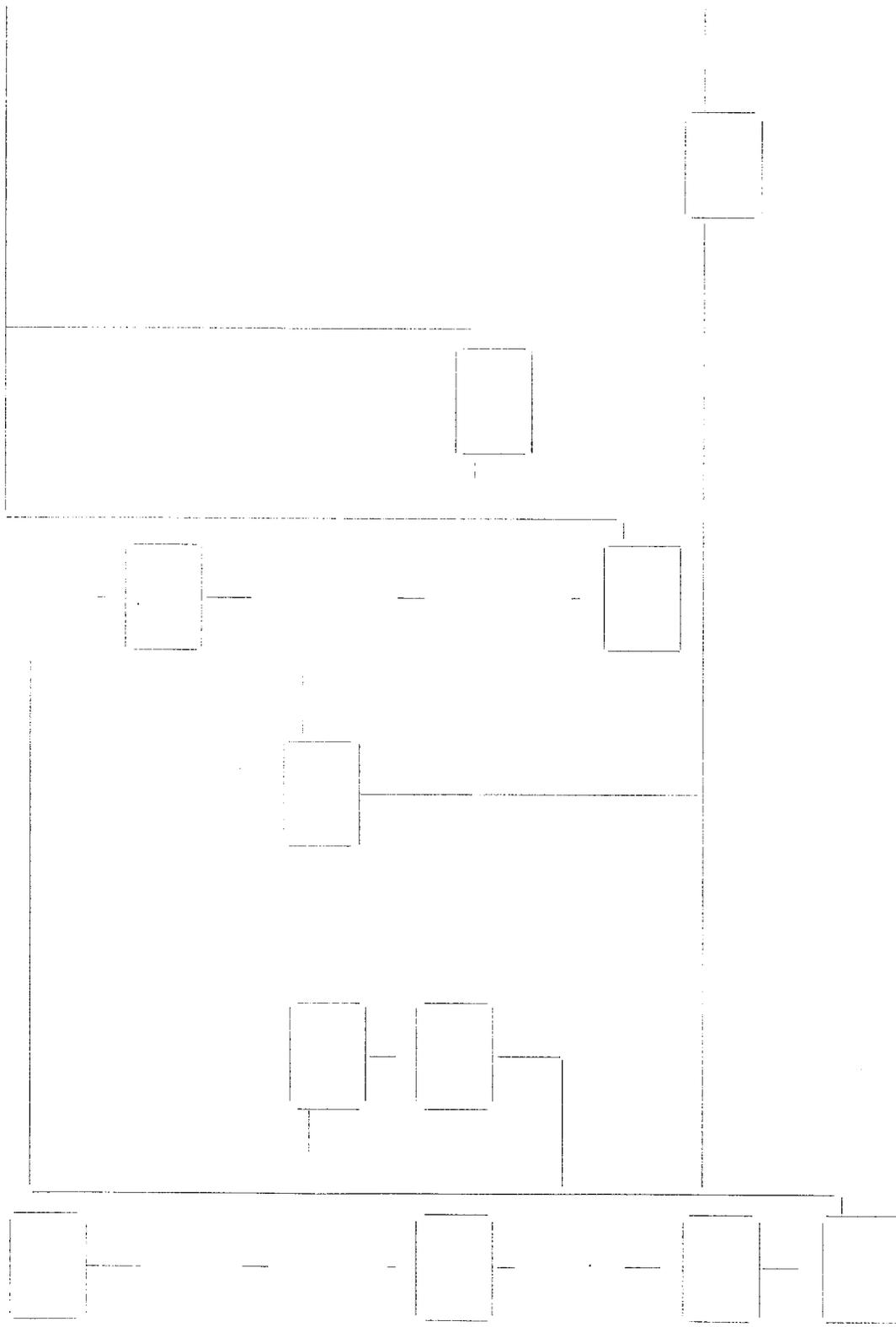
CM Configuration Manager

RP Release Package

IDPM Infrastructure Development Process Model

Step	Task	Responsibility	IDPM Phase
1	Determine deadlines for release	CM, RM, strategic planner	-
	Publicize deadlines	CM	-
2	Identify and submit RC to CM	Client, development staff	1
	Assign RC number to each candidate	CM	1
	Create and maintain RC log	CM	1
3	Define documentation requirements for update/upgrade or maintenance RC	CM	9
	Assignment of documentation writing	CM	9
	Review and approve documentation		9
4	Submit IDPM analysis to CM	developer	1
	Conduct review meetings	CM, others as needed	1
	Approve analysis documentation	CM	1
5	Assign target release number	CM	-
	Notify development staff of analysis documentation approval and target release number	CM	-
	Create and maintain RP log	CM	-
6	IDPM Design Phase	development	2
7	IDPM Testing Phases	development	4 & 6
8	Submit RC and all IDPM documentation to CM	development	7
	Verify sufficient documentation submitted for review	CM	-
9	Conduct documentation review for each RC	CM and others	-
	Approve RC as complete and ready for release management	CM	-
	Reject any incomplete RC, return control to development for revision	CM	-
	Create and maintain RC review log	CM	-
10	Assign final release number to RC	CM	-
	Pass control and documentation of approved RCs to RM	CM	-

Step	Task	Responsibility	IDPM Phase
11	Review RC documentation to gain familiarity and understanding	RM	-
	Assign test plan writing and execution	RM	-
	Maintain activity progress log for RP	RM	-
12	Pass Stand-Alone package to package test step	RM	-
13	Integration test plan documentation is written	Provisioning staff	-
	Test plan approved	RM	-
	Integration test is completed	Provisioning staff	-
	Test results are reviewed	RM	-
	RP approved for package testing	RM	-
14	Package test plan documentation is written	Provisioning staff	-
	Test plan approved	RM	-
	Package test is completed	Provisioning staff	-
	Test results are reviewed	RM	-
	RP approved for pilot testing	RM	-
15	Pilot test plan documentation is written	Provisioning staff	-
	Test plan approved	RM	-
	Pilot test is completed	Provisioning staff	-
	Test results are reviewed	RM	-
	RP approved for deployment	RM	-
	RP rejection sent to CM	RM	-
16	Review rejected package	CM	-
	Redefine requirements	CM	-
	Return control to IDPM for correction	CM	-
17	Release package to IDPM transition support	CM	7



United States
Nuclear Regulatory Commission



Instructions for Preparing Security Plans for Local Area Networks in Compliance With OMB Bulletin No. 90-08

February 1992

Prepared by
National Institute of Standards and Technology
Office of Management and Budget
U.S. Nuclear Regulatory Commission
- Office of Information Resources Management

NUREG/BR-0166



United States
Nuclear Regulatory Commission

Instructions for Preparing Security Plans for Local Area Networks in Compliance With OMB Bulletin No. 90-08

February 1992

Prepared by
National Institute of Standards and Technology
Office of Management and Budget
U.S. Nuclear Regulatory Commission
Office of Information Resources Management

ABSTRACT

This document provides guidelines for U.S. Nuclear Regulatory Commission managers, other staff members, and contractors who are responsible for developing computer security plans for local area networks. It was developed to supplement Office of Management and Budget Bulletin No. 90-08, "Guidance for Preparation of Secu-

ity Plans for Federal Computer Systems That Contain Sensitive Information." Agency managers, network administrators, system users, and security officers should be included when planning for security to ensure that all areas of concerns are considered.

PREFACE

This document provides guidelines for U.S. Nuclear Regulatory Commission managers, other staff members, and contractors who are responsible for preparing security plans for local area networks. It was developed by the National Institute of Standards and Technology to supplement the guidance in Office of Management and Budget (OMB) Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," which mandates security plans but does not address local area networks. The guidelines on how to prepare a security plan for local area networks are to be used by the NRC staff and contractors along with OMB Bulletin No. 90-08. The objectives of these guidelines are to help agency personnel and contractors

- understand the process for preparing a network security plan in conjunction with OMB Bulletin No. 90-08
- reduce the risk and magnitude of harm that could result from the loss, misuse, or unauthorized ac-

cess to or modification of information in NRC networked computer systems

- understand the nature and extent of sensitive information systems and the security requirements for such systems
- understand the adequacy of the administrative, management, and technical approaches used in protecting sensitive systems in networked environments
- understand the responsibilities and accountability for the security of sensitive systems in networked environments
- understand the requirements for additional guidance, standards, assistance, training, and new technology to improve the protection of sensitive information resources.

Contents

ABSTRACT	iii
PREFACE	vii
I. System Identification	1
A. Responsible Organization	1
B. System Name/Title	1
C. System Category	1
D. System Operational Status	1
E. General Description/Purpose	1
F. System Environment and Special Considerations	2
G. Information Contact(s)	2
II. Sensitivity of Information Handled	2
A. Applicable Laws or Regulations Affecting the System	2
B. General Description of Information Sensitivity	2
III. System Security Measures	2
A. Risk Assessment and Management	2
B. Applicable Guidance	2
C. Security Control Measures	3
D. Security Control Measures Status	3
E. Security Control Measures for Major Applications	3
1. Management Controls	3
a. Assignment of Security Responsibility	3
b. Personnel Screening	3
2. Development/Implementation Controls	3
a. Security Specifications	3
b. Design Review and Testing	3
c. Certification	3
3. Operational Controls	4
a. Physical and Environmental Protection	4
b. Production, I/O [Input/Output] Controls	4
c. Emergency, Backup, and Contingency Planning	4
d. Audit and Variance Detection	4
e. Application Software Maintenance Controls	5
f. Documentation	5
4. Security Awareness and Training	5
a. Security Awareness and Training Measures	5
5. Technical Controls	5
a. User Identification and Authentication	5
b. Authorization/Access Controls	6
c. Data Integrity/Validation Controls	6

d.	Audit Trails and Journaling	6
6.	Complementary Controls Provided by Support Systems	6
F.	Security Control Measures for General Support Systems	6
1.	Management Controls	6
a.	Assignment of Security Responsibility	6
b.	Risk Analysis	6
c.	Personnel Screening	6
2.	Acquisition/Development/Installation Controls	6
a.	Acquisition Specifications	6
b.	Accreditation/Certification	7
3.	Operational Controls	7
a.	Physical and Environmental Protection	7
b.	Production, I/O [Input/Output] Controls	7
c.	Emergency, Backup, and Contingency Planning	7
d.	Audit and Variance Detection	7
e.	Hardware and System Maintenance Controls	8
f.	Documentation	8
4.	Security Awareness and Training	8
a.	Security Awareness and Training Measures	8
5.	Technical Controls	8
a.	User Identification and Authentication	8
b.	Authorization/Access Controls	8
c.	Integrity Controls	9
d.	Audit Trail Mechanisms	9
e.	Confidentiality Controls	9
6.	Controls Over the Security of Applications	9
IV.	Additional Comments	9
	Appendix A—Sample Security Plan For A Local Area Network	A-1
	Appendix B—OMB Bulletin No. 90-08, "Guidance For Preparation Of Security Plans For Federal Computer Systems That Contain Sensitive Information"	B-1

Instructions For Preparing Security Plans For Local Area Networks In Compliance With OMB Bulletin No. 90-08

This document is to be used as a companion document to Office of Management and Budget (OMB) Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," when preparing a computer security plan for a local area network (LAN). A sample LAN security plan is included as Appendix A to this document; OMB Bulletin No. 90-08 is reproduced in Appendix B.

I. System Identification

This section of the LAN security plan should contain basic identifying information.

A. Responsible Organization

Name the organization that is responsible for ensuring network continuity. State if this network is run by a contractor or State agency.

B. System Name/Title

The title should be meaningful and should describe the system, keeping in mind the organization's mission. This title is not always what users or operators call the system (e.g., the LAN). It should be descriptive of the kind of processing that is done (e.g., personnel/payroll LAN).

C. System Category

Most networks will be categorized as general support systems; however, some networks can be major application systems.

Major Application: A major application system performs a clearly defined function for which there are readily identifiable security considerations and needs.

- Is the network dedicated to one application? Is the network managed as a part of the application?

General Support System: A general support system consists of hardware and software that provide general automated data processing (ADP) or network support for a variety of users and applications.

- Does this network provide general ADP support for a variety of users and applications? If none of the applications are sensitive, perhaps the support system itself may be considered sensitive.

D. System Operational Status

Describe the operational status of the network (i.e., operational, under development, or undergoing a major modification).

E. General Description/Purpose

Provide a brief description of the function and purpose of this network. Include a concise description of the type of information that is handled by this network.

- What kind of information does this network contain or transmit (e.g., project data, personnel data)?
- What is the nature of the applications (i.e., what is this network used for)?
- Have the security requirements been coordinated between the users and network management (i.e., has the network security officer polled the users to determine what types of security requirements are needed)?

F. System Environment and Special Considerations

Provide a general description of the technical system. Include environmental concerns. Describe the operating and applications software.

- How is the operating and applications software licensed (i.e., site wide, multiple user, single user)?
- Is the network located in an office building, in a computing facility, or off site?
- Are there any special conditions such as high-traffic areas, water damage, or earthquakes? Is this network located in a harsh or overseas environment?
- Is this network connected to any public lines or networks? Is there any dial-up capability?
- What equipment does this network consist of (e.g., personal computers, minicomputers, mainframes)?
- What is the network operating system? What are the software packages that run on this network? Are these packages off-the-shelf or custom-made software?
- Who are the users of this network (i.e., is it used within the agency, between agencies, by contractors, by the general public, by foreign nationals)?

Instructions

- Are there any other types of interfaces with other Federal and non-Federal systems?

G. Information Contact(s)

Provide the name, title, organization, and telephone number of one or more persons designated to be the point of contact for this network. This contact must be knowledgeable enough to provide additional information regarding the use and security of this network if needed (e.g., systems administrator, security officer).

II. Sensitivity of Information Handled

This section should contain a description of the types of information handled by this system and thus provide the basis for the system's security requirements. The following should be included:

A. Applicable Laws or Regulations Affecting the System

Examples are the Privacy Act and the Financial Managers Integrity Act.

B. General Description of Information Sensitivity

The information stored on and transmitted by this network should be addressed in accordance with OMB Bulletin No. 90-08.

A system may need protection for one or more of the following reasons:

- Confidentiality: The need to protect information from intentional and unintentional disclosure (e.g., personal data, proprietary information).
 - Does this network store or transmit information such as Social Security numbers, medical information, financial information, time release critical information?
- Integrity: The need to protect information from intentional and unintentional modification (e.g., financial information, scientific research information).
 - Does this network store or transmit life-threatening information (e.g., air traffic control information, hazardous weather conditions)?
 - Does this network store or transmit such information that if its accuracy were not protected, the agency's mission could not be accomplished?

- Is this network used for scientific or medical research where the information needs to be as accurate as possible (e.g., pharmaceutical testing information, cancer research data)?
- Availability: The need to protect information from intentional and unintentional loss (e.g., air traffic control information, payment dissemination).
 - Does this network store or transmit information that needs to be available in a timely manner (e.g., census information, air traffic control information)?
 - Would the unavailability of this network cause a loss of life, monetary loss, failure of the agency's mission, or embarrassment to the Government?
 - How long can this office function without the use of this network?

For each category (confidentiality, integrity, and availability), indicate a protection requirement of high, medium, or low.

III. System Security Measures

This section should contain a description of the control measures. To ascertain which controls and procedures are needed to protect this network, threats and vulnerabilities need to be assessed.

A. Risk Assessment and Management

Risk assessment and management are crucial elements of the security planning process.

- Has a risk analysis of this network ever been performed? If so, describe the methodology used.

B. Applicable Guidance

Provide a list of specific standards or other guidance that was used in the design, implementation, or operation of the protective measures used on this network.

- What standards or guidelines were used in the design, implementation, or operation of the protective measures that are used on this network (e.g., encryption keys, data authentication, key management, NRC computer security policy documents)?
- Was any policy, guideline, or standard developed by the NRC used in the implementation, design, or operation of the network security measures?

C. Security Control Measures

There are two sets of controls: one for major applications and one for general ADP support systems. Because

networks tend to be general support systems, Section F will most likely be used. If the network is a major application, use Section E. State whether the controls are in place, planned, in place and planned, or not applicable. For the planned controls, give the date when these controls will be implemented. It is also helpful to the network manager and users to describe these control measures.

D. Security Control Measures Status

For each of the control measures in Sections E and F, specify if it is (1) in place, (2) planned, (3) in place and planned, or (4) not applicable.

E. Security Control Measures for Major Applications

1. Management Controls

These controls are used for the overall management of the network as a major application. They include authorization, personnel screening, risk management, and assignment of security responsibility.

a. *Assignment of Security Responsibility*

The assignment of security responsibility is important to ensure that security is considered. The person assigned this responsibility should be responsible for all aspects of the security of the network.

- Who is responsible if something goes wrong? Has the responsibility for the security of this network been assigned? This responsibility should NOT be assigned to the network administrator. Often if the network administrator and security officer are the same, security is overlooked to keep the network running.

b. *Personnel Screening*

Personnel screening should be in place. This screening should include making sure only personnel with a need to know have access to the network.

- Have personnel had background checks?
- Does anyone who can access the network need to be screened?

2. Development/Implementation Controls

These controls ensure that protection is built into the network, especially during network development.

a. *Security Specifications*

Security specifications should be in place for the appropriate technical, administrative, physical, and personnel security required for networks.

- Are the appropriate technical specifications in place for this network?
- Do these technical specifications include security for shared file access such as file locking and record locking?
- Is a password management system in place?
- Are controls in place for personnel security? Are appropriate personnel procedures and policies in place?

b. *Design Review and Testing*

A design review and systems test should be completed before this major application network is in operation. The review and test are needed to ensure that the major application network meets the security specifications. Full documentation of this design review and test should be kept and maintained.

- Have a design review and test been completed? Do the results show that the major application network meets the security specifications required?

c. *Certification*

Networks should be certified in accordance with OMB Bulletin No. 90-08.

- Has management authorized this network for sensitive processing? This may include any constraints placed on processing, such as no processing during nonwork hours or no use of dial-up lines.

3. Operational Controls

These controls include the day-to-day procedures and mechanisms that are used to protect the operational application networks.

Instructions

a. *Physical and Environmental Protection*

These controls provide for the physical and environmental protection of the network, including all physical protection devices such as fire extinguishers, locks, or video cameras.

- Are controls in place to protect this network against physical and environmental threats and hazards?
- Is this network housed in an office building with doors that can be locked? Are any switches or terminals accessible to unauthorized personnel?
- Is there 24-hour guard service?
- Is proper firefighting equipment available?
- Are proper water detection devices along with means to eliminate excess water available?
- Are fire, heat, and smoke detectors in place?
- Are uninterruptible power supplies or electrical surge protectors available?

b. *Production, I/O [Input/Output] Controls*

These controls provide for the proper handling, processing, storage, and disposal of the input and output of the network.

- Are controls in place to manage the input and output? This includes the storage and disposal of printouts and floppy diskettes or other media on which information is stored or data screening.
- Are input and output media properly labeled (e.g., labels stating "project x,y,z" or "sensitive")?

c. *Emergency, Backup, and Contingency Planning*

These controls include the measures that are to be used to ensure continuity of support in the event of a network failure.

- Are the appropriate emergency, backup, and contingency plans in place for this network?

- Are these plans readily available for the network manager and users in case of an emergency? These plans should ensure the continuity of support in the event of a network failure.
- Is there an alternative network that could be used in case of an emergency?
- Can the duties of this office be performed manually in case of an emergency?

d. *Audit and Variance Detection*

These controls allow management to conduct independent reviews of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures. Variance detection checks for anomalies in such items as numbers and types of transactions and volume and dollar thresholds, and other deviations from standard activity profiles.

- Are there controls that will allow management to conduct an independent review of the systems records and activities? The purpose of this review should be to test the adequacy of network controls and to detect and react to departures from established procedures, policies, and rules.
- Are there sign-in and sign-out logs for those who have physical access to the network server?
- Are job request forms necessary? If so, are they used?
- Is there a mechanism to monitor the network load and number of access attempts?
- Is there any software residing on this network that monitors for viruses or other anomalies?

e. *Application Software Maintenance Controls*

These controls are used to monitor application software installation and updates. They ensure that the software functions as expected and that a historical record of application system changes is maintained.

- Are controls in place to monitor the application software updates?

- Is there a software configuration policy? If so, who authorizes the software changes and updates?
- Is a record kept and maintained regarding the software changes and updates? If so, is this record available to the appropriate personnel when it is needed?
- Are virus-protection products used to check if application software has been modified?

f. *Documentation*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are there descriptions of the hardware and software, policies, and procedures related to the computer security of the network? These should include backup and contingency plans for the network and a description of the operator procedures.
- Are there descriptions of the network layout, software, hardware, and configuration or cable charts?
- Are there descriptions of the end-user procedures regarding proper handling of sensitive data?
- Are these descriptions readily available to all who need access to them?
- Are there any maintenance contracts regarding this network? Are they accessible to the personnel who need them?

4. Security Awareness and Training

a. Security Awareness and Training Measures

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Is a security awareness and training course for users, technical staff, and managers in place?
- What is included in this training course?
- Does this training address specific network issues, such as the protection of passwords?

- How often is this course offered?
- Do all employees have to attend this course periodically?
- Is security covered in any other ADP training such as WordPerfect, dBase, or Lotus 1,2,3?

5. Technical Controls

This section should be completed in accordance with OMB Bulletin No. 90-08.

Most of the following controls are found within the network operating system and should be described in the network operating system documentation.

a. *User Identification and Authentication*

These controls are used to verify the identity of a station, originator, or individual before allowing access to the network. They are the basis for authorization and access controls.

- Is user identification required to access this network?
- Does this network pass this identification to other networks that are connected?
- Are passwords, tokens, or other mechanisms used to authenticate the identity of a user (e.g., encryption keys, fingerprints, voice or signature authentication) before access to the network is granted?

b. *Authorization/Access Controls*

These controls are used to detect and/or permit only authorized access to or within the network.

- Does the operating system offer controls to restrict access to the operating system? If not, are any controls developed by the NRC in place?
- Are any hardware or software features used to detect and/or permit only authorized access to or within the system used (e.g., access lists)?
- Are there limits on access to computer programming resources?
- Does the operating system have built-in authorization and access controls

Instructions

that can be adjusted to allow or disallow reading, writing, or executing files and programs?

c. *Data Integrity/Validation Controls*

These controls protect the operating system, application system, and information from alteration or destruction.

- Are any controls in place that provide message authentication?

d. *Audit Trails and Journaling*

These controls provide monitoring and recording capabilities to retain a chronological record of system activities.

- Is there an audit trail mechanism to record and monitor network activity (e.g., system log)?
- Can this mechanism be used to reconstruct the activities of the network when a problem is detected?

6. Complementary Controls Provided by Support Systems

F. Security Control Measures for General Support Systems

1. Management Controls

These controls are used for the overall management of the network. They include authorization, personnel screening, risk management, and assignment of security responsibility.

a. *Assignment of Security Responsibility*

The assignment of security responsibility is important to ensure continuity of network operations. The person assigned this responsibility should be responsible for all aspects of the security of the network.

- Who is responsible if something goes wrong? Has the responsibility for the security of this network been assigned? This responsibility should NOT be assigned to the network administrator. Often if the network administrator and security officer are the same, security is overlooked to keep the network running.

- Is there a checksum capability within the operating system that allows files to be checked after transmission to ensure the correct number of bytes was transferred?

- Is an error-checking or error-correcting technique used?

- Is nonrepudiation available?

b. *Risk Analysis*

Many risk analyses do not address networks directly.

- Did the risk analysis that was used address the network directly?

c. *Personnel Screening*

Personnel screening should be in place. This screening should include making sure only personnel with a need to know have access to the network.

- Have personnel had background checks?
- Does anyone who can access the network need to be screened?

2. Acquisition/Development/Installation Controls

These controls ensure that adequate security is built into and maintained in the network to minimize the damage that could occur as a result of threats and vulnerabilities.

a. *Acquisition Specifications*

Security should be included in the acquisition specifications for a network. It is less expensive to have security built into the network from the beginning. When adding security to an already existing network, many vulnerabilities may be overlooked.

- Was security included in the life cycle of the development model?
- Have the appropriate specifications been considered in the technical, administrative, physical, and personnel security areas?
- Do all the contracts for the procurement of computer hardware, software, and services for this network include a

specification for security requirements?

b. *Accreditation/Certification*

Networks should be accredited and certified in accordance with OMB Bulletin No. 90-08.

- Has management authorized this network for processing sensitive information? This may include any constraints placed on processing, such as no processing during nonworking hours or no use of dial-up lines.

3. Operational Controls

These controls should include physical and environmental protection, emergency backup systems, contingency planning, audit and variance detection, maintenance of application software, documentation, and a periodic check for viruses.

a. *Physical and Environmental Protection*

These controls provide for the physical and environmental protection of the network, including all physical protection devices such as fire extinguishers, locks, or video cameras.

- Are controls in place to protect this network against physical and environmental threats and hazards?
- Is this network housed in an office building with doors that can be locked. Are any switches or terminals accessible to unauthorized personnel?
- Is there 24-hour guard service?
- Is proper firefighting equipment available?
- Are proper water detection devices along with means to eliminate excess water available?
- Are fire, heat, and smoke detectors in place?
- Are uninterruptible power supplies or electrical surge protectors available?

b. *Production, I/O [Input/Output] Controls*

These controls provide for the proper handling, processing, storage, and disposal of the input and output of the network.

- Are controls in place to manage the input and output? This includes the storage and disposal of printouts and floppy diskettes or other media on which information is stored or data screening.
- Are input and output media properly labeled (e.g., labels stating "project x,y,z" or "sensitive")?

c. *Emergency, Backup, and Contingency Planning*

These controls include the measures that are to be used to ensure continuity of support in the event of a network failure.

- Are the appropriate emergency, backup, and contingency plans in place for this network?
- Are these plans readily available for the network manager and users in case of an emergency? These plans should ensure the continuity of support in the event of a network failure.
- Is there an alternative network that could be used in case of an emergency?
- Can the duties of this office be performed manually in case of an emergency?

d. *Audit and Variance Detection*

These controls allow management to conduct independent reviews of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures. Variance detection checks for anomalies in such items as numbers and types of transactions and volume and dollar thresholds, and other deviations from standard activity profiles.

- Are there controls that will allow management to conduct an independent review of the systems records and activities? The purpose of this review should be to test the adequacy of network controls and to detect and react to departures from the established procedures, policies, and rules.

Instructions

- Are there sign-in and sign-out logs of those who have physical access to the network server?
- Are job request forms necessary? If so, are they used?
- Is there a mechanism to monitor the network load and number of access attempts?
- Is there any software residing on this network that monitors for viruses?

e. *Hardware and System Maintenance Controls*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are controls in place to monitor the installation of software updates? These controls include keeping a historical record of the system changes and ensuring that only authorized software is installed on the network.
- Is there a record of all installations and modifications of software and hardware?
- Is the software and hardware tested before the real-time use of the system goes into effect?

f. *Documentation*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are there descriptions of the hardware and software, policies, and procedures related to the computer security of the network? These should include backup and contingency plans for the network and a description of the operator procedures.
- Are there descriptions of the network layout, software, hardware, and configuration or cable charts?
- Are these descriptions readily available to all who need access to them?
- Are there any maintenance contracts regarding this network? Are they accessible to the personnel who need them?

4. Security Awareness and Training

a. *Security Awareness and Training Measures*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Is a security awareness and training course for users, technical staff, and managers in place?
- What is included in this training course?
- Does this training address specific network issues, such as the protection of passwords?
- How often is this course offered?
- Do all employees have to attend this course periodically?

5. Technical Controls

Most of the following controls are found within the network operating system and should be described in the network operating system documentation.

a. *User Identification and Authentication*

These controls are used to verify the identity of a station, originator, or individual before allowing access to the network. They are the basis for authorization and access controls.

- Is user identification required to access this network?
- Does this network pass this identification to other networks that are connected?
- Are passwords, tokens, or other mechanisms used to authenticate the identity of a user (e.g., encryption keys, fingerprints, voice or signature authentication) before access to the work is granted?

b. *Authorization/Access Controls*

These controls are used to detect and/or permit only authorized access to or within the network.

- Does the operating system offer controls to restrict access to the operating system? If not, are any controls developed by the NRC in place?

- Are any hardware or software features used to detect and/or permit only authorized access to or within the system used (e.g., access lists)?
- Are there limits on access to computer programming resources?
- Does the operating system have built-in authorization and access controls that can be adjusted to allow or disallow reading, writing, or executing files and programs?

c. *Integrity Controls*

These controls protect the operating system, application system, and information from alteration or destruction.

- Are any controls in place that provide message authentication?
- Is there a checksum capability within the operating system that allows files to be checked after transmission to ensure the correct number of bytes was transferred?
- Is an error-checking or error-correcting technique used?
- Is nonrepudiation available?

d. *Audit Trail Mechanisms*

These controls provide monitoring and recording capabilities to retain a chronological record of system activities.

- Is there an audit trail mechanism to record and monitor network activity (e.g., system log)?
- Can this mechanism be used to reconstruct the activities of the network when a problem is detected?

e. *Confidentiality Controls*

These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. They may provide data protection at the user site, at the computer facility, in transit, or some combination of these.

- Is encryption used to ensure confidentiality during storage or transmission?
- Are any other technical means used to protect confidentiality?

6. *Controls Over the Security of Applications*

The security of each application that is processed on a support system could affect the security of all others processed on that same system.

- Is the manager of the network aware of the security requirements of the applications that are processed? The manager should understand the risk that each application represents to the overall system.
- Are the network users and applications owners aware of what the network does and does not do to protect sensitive data?

IV. Additional Comments

This section is intended for additional comments about the security of this network and any perceived need for guidance or standards.

- Is there anything else of importance about the security of this network that was not covered in the preceding sections?
- Is any additional security guidance or security standard needed that would ensure that this network operates more efficiently?

APPENDIX A

Sample Security Plan For A Local Area Network

APPENDIX A SAMPLE SECURITY PLAN FOR A LOCAL AREA NETWORK

The following is a sample security plan for a local area network (LAN) that follows OMB Bulletin No. 90-08 and the guidelines developed by the National Institute of Standards and Technology. The following entries should be included in this security plan.

I. SYSTEM IDENTIFICATION

A. Responsible Organization

U.S. Nuclear Regulatory Commission

Branch: _____

Office: _____

B. System Name/Title

System A.

C. System Category

Major application.

D. System Operational Status

Operational.

E. General Description/Purpose

The immediate and primary continuing purpose of System A is to limit the consequences of incidents at nuclear power reactors. It is used to recommend to State and local authorities whatever actions may be necessary to protect the public and the environment. The NRC, through independent assessments and support where necessary, adds a safety factor to help ensure that the protective measures being recommended are adequate.

System A consists of three microcomputer-based subsystems: (1) LAN 1, (2) LAN 2, and (3) personal computer (PC) workstations.

LAN 1 includes workstations throughout the System A area. It is used to run models, exchange information, and send summary reports to other organizations. It also backs up LAN 2.

LAN 2 is the primary support for routine functions at all hours in the System A area. It contains all of the programs needed by system A personnel to compile periodic summaries and plant status reports. The PC workstation subsystem comprises several stand-alone workstations within

and outside the System A area that are not connected to the LAN.

F. System Environment and Special Considerations

LAN 1 and LAN 2 are fully contained within the System A area and require an access code on a keycard to open the door. All LAN servers are kept in a locked room that is closely monitored. Only authorized personnel are issued keys to the room.

G. Information Contact

John Doe, Chief, Office of _____, (xxx) xxx-xxxx

II. SENSITIVITY OF INFORMATION HANDLED

A. Applicable Laws or Regulations Affecting the System

Information maintained in this system is covered by the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, and NRC's regulations in 10 CFR Part 9.

B. General Description of Information Sensitivity

Confidentiality of data—Primary concern

Integrity of data—Primary concern

Availability of data—Primary concern

C. Need for Protective Measures

The information that is stored on System A's PC workstations is personnel information, that is, employees' Social Security numbers, grades, addresses, telephone numbers, and birth dates. This type of information is considered sensitive. For this reason, the system is considered to be sensitive unclassified. No sensitive information is stored on the LAN. Sensitive information should NEVER be stored on the LAN.

D. Estimated Risk

Because of the sensitive information that is stored in System A, the estimated risk of disclosure with regard to integrity, availability, and confidentiality would be a primary concern.

E. Protection Requirement

The System A PCs and LANs must maintain "high" confidentiality and "high" integrity for all identifiers such as Social Security numbers, grades, birth dates, and home telephone numbers because unauthorized access could mean loss of privacy for individuals. The System A LANs must maintain "high" availability because they support continuous organizational functions.

III. SYSTEM SECURITY MEASURES

A. Risk Assessment and Management

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) performed a formal risk analysis of System A in 1985. The Office of Information Resources Management, Codes and Standards Section, performed a risk analysis of the system in 1990, using the Los Alamos Vulnerability Analysis Tool to determine the vulnerabilities in the system and ways to correct them.

B. Applicable Guidance

NRC Appendix 2301, "Security of Automated Information Systems," dated July 25, 1985, Part II, paragraph A.1, addresses the requirement for unclassified systems processing sensitive or sensitive unclassified data. The Privacy Act, mentioned in Section II.A, also applies. The Computer Security Act of 1987 does not apply.

C. Security Control Measures (According to OMB Circular No. A-130)

Specific control measures are in place for System A to ensure that management of the system is being monitored. These control measures adhere to the requirements specified in the Computer Security Act of 1987; OMB Circular No. A-130, Appendix III, "Management of Federal Information Resources"; and applicable Federal Information Processing Standards and Special Publications produced by NIST.

D. Security Control Measures Status

Specific management, operational, and technical measures that are in place, planned, in place and planned, or not applicable are described in Section E of this plan for System A.

E. Security Control Measures for Major Applications

1. Management Controls—In place

- a. *Assignment of Security Responsibility*—In place.

The duties of system security officer have been assigned to John Doe, Office of Supply, (xxx) xxx-xxxx. The duties of assistant security officer have been assigned to Jane Doe, Office of Supply, (xxx) xxx-xxxx.

- b. *Personnel Screening*—In place.

All agency personnel involved in the use, design, development, operation, or maintenance of System A undergo a background investigation. In addition, agency personnel and contractors must meet the requirements for Federal employees and contractors found in Office of Personnel Management Federal Personnel Manual Chapters 731, 732, and 736.

2. Development/Implementation Controls—In place.

- a. *Security Specifications*—In place where applicable.

Operational security requirements have been defined for system developers. System A and System B (backup to System A) are being completed under contracts that specify the requirements; System A is composed largely of off-the-shelf components, including software, that are selected and integrated to meet operational requirements.

- b. *Design Review and Testing*—In place where applicable.

System A design reviews have been completed.

- c. *Certification*—In place where applicable.

The Office of Information Resources Management has approved System A designs.

3. Operational Controls—In place.

- a. *Physical and Environmental Protection*—In place.

Access to the System A area is controlled by keycard doors.

- b. *Production, I/O [Input/Output] Controls*—Not applicable.

- c. *Emergency, Backup and Contingency Planning*—In place.

Computer programs and data are backed up or are available at more than one location in the event of a localized problem. A tape backup is being installed on System A, because the system may, at times, contain information that is not duplicated elsewhere. Systems in the System A area are designed with either a system of workstation uninterruptible power supplies and mirrored external drives or mutual backup in the event of a workstation failure. A roof-mounted diesel generator automatically delivers power for equipment, telephones, and lighting if there is a major loss of power. In case of a more widespread problem, procedures to rely on paper forms and other communications that were used before computers were available are in place and have been tested. A complete contingency plan is being developed.

d. *Audit and Variance Detection*—In place.

Only one function of System A lends itself to "standard activity profiles." Costs, access times and duration, activities, and other audit factors are monitored by the office responsible for the commercial electronic message service used to support emergency response functions.

e. *Application Software Maintenance Controls*—In place.

System A software is standard for all users. One person approves functional modifications, and other designated persons implement and test the modifications to ensure that they do not have unintended operational effects. In addition, two persons are responsible for ensuring that any workstation will function as required at any time. The latest software versions are documented. Similar requirements apply to other System A subsystems.

f. *Documentation*—In place.

The Office of Information Resources Management (IRM) maintains security-related policies, standards, and other policies. The IRM LAN manager maintains LAN system documentation. IRM personnel maintain application documentation, user procedures, and a mailing list of persons to contact to address various problems.

4. *Security Awareness and Training*—In place.

Specific security measures that relate to specific applications are included with user procedures (e.g., changing passwords); these measures will be reviewed and improved as necessary on the basis of this security plan.

5. *Technical Controls*—In place.

a. *User Identification and Authentication*—In place.

LAN equipment requires an assigned account and six-character passwords for access to computer programs.

b. *Authorization/Access Controls*—In place.

System A data and programs can be changed only from a single workstation located in the LAN area. All LAN workstations can use only the programs for which a LAN manager has granted access.

c. *Data Integrity/Validation Controls*—In place.

System A data are checked during transmission. Computer programs are backed up using highquality, off-the-shelf software, and data from these programs are generally used only temporarily and stored on diskettes or tapes that are physically protected while the data are being used. Messages between the System A area and the rest of the world are stored on the protected computers of the commercial electronic message service or arrive via fax (hard copy) in the System A area. The procedure for exchanging messages in any medium requires authentication of the source and verification of certain data via telephone to a number arranged in advance.

d. *Audit Trails and Journaling*—In place.

LAN software maintains records of activities, as do the commercial data bases. The electronic message service also notifies any user if unsuccessful attempts have been made to log in.

6. *Complementary Controls Provided by Support Systems*—In place.

All users of System A who support daily activities receive regular specialized training tailored to their roles. One result is that users quickly spot anything that differs from what they have been trained to expect. Members of the staff who are responsible for System A development, maintenance, and training can then use their knowledge of and experience

with the system to identify possible security problems.

F. Security Control Measures for General Support Systems

Not applicable. If the system is a general support system (a system used by many users in different locations within the same organization), the information called for in Section F of Appendix A to OMB Bulletin No. 90-08 and the NIST guidelines should be supplied instead of that called for in Section E.

IV. ADDITIONAL COMMENTS

Because both staff and computer security are involved, both the NRC Office of Security and the computer security staff in the Office of Information Resources Management will review this security plan.

APPENDIX B

**OMB Bulletin No. 90-08, "Guidance For Preparation Of Security Plans For
Federal Computer Systems That Contain Sensitive Information"**



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 9, 1990

THE DIRECTOR

OMB Bulletin No. 90-08

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

1. **Purpose.** The purpose of this Bulletin is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. This Bulletin supersedes OMB Bulletin No. 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information" (July 6, 1988).

2. **Authority.** The Computer Security Act of 1987 ("The Act") (P.L. 100-235), requires Federal agencies to identify each computer system that contains sensitive information and to prepare and implement a plan for the security and privacy of these systems. The Act further requires agencies to submit copies of those plans to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for advice and comment, and it makes such plans subject to OMB disapproval.

3. **Objectives of the Security Planning Process.** The security planning process is designed to reduce the risk and magnitude of harm that could result from the loss, misuses or unauthorized access to or modification of information in Federal computer systems. This process is intended to help agencies identify and assess:

- a. the nature and extent of sensitive information systems and the security requirements of such systems;
- b. the adequacy of the administrative, management, and technical approaches used in protecting sensitive systems;
- c. responsibilities and accountability for the security of sensitive systems; and
- d. requirements for additional guidance, standards, assistance, training, and new technology to improve the protection of sensitive information resources.

4. **Applicability.** This Bulletin applies to Federal agencies as defined in Section 3(b) of the Federal Property and Administrative Services Act of 1949, as amended. The Bulletin does not apply to agency operation of systems that contain classified information, systems involving intelligence activities, cryptologic activities related to national security, or direct command and control of military forces. The Bulletin also does not apply to equipment that is integral to a weapons system or direct fulfillment of military or intelligence missions (excluded by 10 U.S.C. 2315). In addition, it does not apply to mixed classified/unclassified systems, if such systems are always operated under rules for protecting classified information.

5. **Changes from OMB Bulletin No. 88-16.**

- a. This year's effort will focus on implementation of security plans.
- b. There will be site visits to the departments and agencies to discuss their computer security programs and identify and fix deficiencies in those programs.
- c. New security plans are not required for all systems. Plans are only required for new systems and those for which an acceptable plan was not previously reviewed.
- d. Guidance for preparing individual plans is revised and expanded based on last year's experience.

6. **Action Required.**

- a. Every agency must implement security plans for systems which contain sensitive information, incorporating appropriate advice and comment from NIST/NSA.
- b. Every agency must prepare a new computer security plan for each system that contains sensitive information, if:
 - (1) the system is new or significantly modified; or
 - (2) a plan for the system was not previously sent to NIST/NSA for advice and comment (particular emphasis should be on contractor, State, and local systems operated on behalf of the agency to perform a Federal function); or
 - (3) staff members of NIST/NSA advised the agency they were unable to provide advice and comment on the previous plan for the system.

These plans should be consistent with the format shown in Appendix A. Alternative formats may be used, provided

they contain, at a minimum, the information described in Appendix A.

- c. Every agency must establish a process to ensure that independent advice and comment on each plan developed in accordance with Section 6.b, above, is provided. Such advice and comment should be provided prior to developing a new system or significantly modifying an existing system.
- d. Every agency must ensure that security plans incorporate appropriate internal control corrective actions identified pursuant to OMB Circular No. A-123.
- e. Every agency must prepare materials as described in Section 8, meet with OMB, NIST, and NSA staff as described in Section 7, and work with NIST and NSA to improve agency computer security.

7. Assistance Visits.

- a. Agencies will be scheduled for visits by OMB, NIST, and NSA staff. The purpose of these visits will be for OMB to discuss the agency's implementation of the Act. NIST and NSA will provide technical advice and assistance on the agency's security needs as requested.
- b. Among the items to be discussed will be:
 - (1) The completeness of identification of sensitive computer systems;
 - (2) The quality, scope, and thoroughness of security plans;
 - (3) Any internal control weaknesses identified pursuant to OMB Circular No. A-123 related to computer systems, and plans for addressing those weaknesses;
 - (4) For agencies subject to OMB Bulletin No. 89-17, "Federal Information Systems and Technology Planning" their response to that Bulletin;
 - (5) Material available in accordance with Section 8, below.
- c. Agencies should also be prepared to discuss the approach that is being taken to ensure that computer security plans for new or modified computer systems are prepared and reviewed.

8. Material for Meetings. Agencies should, at a minimum, have

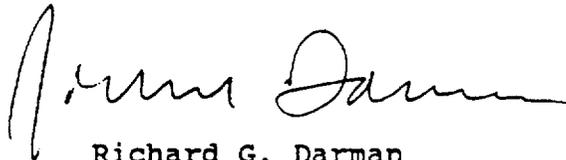
Appendix B

the following information available:

- a. agency-wide computer security policies and a summary of agency computer security procedures, standards, and requirements;
- b. agency assignment of responsibilities for implementation and operation of the security program;
- c. the agency management plan for ensuring implementation of system computer security plans that includes a description of:
 - (1) the involvement of agency management,
 - (2) how computer security plans are being integrated into information resources management plans,
 - (3) the approach for ensuring that funds, personnel and equipment are planned for and budgeted, and
 - (4) the implementation schedule;
- d. the method used to identify the agency's sensitive systems;
- e. any known agency needs for guidance or assistance.

9. **Information Contacts.** Questions regarding Appendix A and other specific plan preparation guidance should be addressed to Jon Arneson (301 975-3870). Questions concerning other aspects of this Bulletin may be directed to Ed Springer (202 395-4814.)

10. **Expiration.** This Bulletin will remain in effect until it is superseded by a revision to OMB Circular No. A-130 and incorporated into standards or guidelines to be issued by NIST.



Richard G. Darman
Director

Attachment

OMB BULLETIN NO. 90-08
APPENDIX A

INSTRUCTIONS FOR PREPARING SYSTEM SECURITY PLANS

GENERAL

The objective of computer security planning is to improve protection of information and information processing resources. In order for plans for the protection of the resources to be adequate, the managers most directly affected by and interested in the information or processing capabilities must be comfortable that their information and/or processing capabilities are adequately protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities.

The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. Thus it should reflect input from various managers with responsibilities concerning the system, including functional "end users" or information owners, the system operator and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the elements described below are adequately covered and are readily identifiable.

It should be noted that plans for the security of contractor, State, and local systems that perform a Federal function may be significantly different from plans for Federally operated systems. The plans for such systems are Federal plans for actions intended to ensure against the risk of loss or harm from the Federal government's perspective. Thus, such plans might not require descriptions of specific developmental, operational, or technical controls as described in this Appendix, but of controls measured by functional performance criteria (e.g., limits on errors or requirements for certain levels of accuracy). The key in identifying such systems and planning for their security is to determine Federal risk and assess the best way to "insure" against that risk.

Each security plan for a Federally operated system should have four basic sections:

- I System Identification
- II Sensitivity of Information
- III System Security Measures
- IV Additional Comments

The remainder of this Appendix contains a description of the scope, content, and format of each of the four sections.

I. SYSTEM IDENTIFICATION

This section of the plan contains basic identifying information about the system.

A. Responsible Organization - The specific Federal organizational subcomponent responsible for the system being reported. If a State or local government or contractor is actually performing the function, identify both the Federal and other organization and describe the relationship.

B. System Name/Title - Logical boundaries must be drawn around the various processing, communications, storage, and related resources to define a system. For planning purposes, those systems in an agency or its subordinate elements under the same direct management control with essentially the same function, characteristics, and security needs may be treated as a single system. Each system name/title should be both meaningful and distinct from other system names/titles.

C. System Category - Categorize each system as either a major application, or as a general support system, in line with the primary management responsibility for the system.

- **Major application** - These are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components.

- **General support system** - These consist of hardware and software that provide general ADP or network support for a variety of users and applications. Individual applications may be less easily distinguishable than in the previous category, but such applications may contain sensitive information. Even if none of the individual applications are sensitive, however, the support system itself may be considered sensitive if overall, the aggregate of applications and support provided are critical to the mission of the agency.

D. System Operational Status - One of the following:

- o Operational - system is currently in operation.
- o Under development - system is currently under design, development, or implementation.
- o Undergoing a major modification - system is currently undergoing a major conversion or transition.

If the system is either under development or undergoing a major modification, provide information about methods being used to assure that up-front security requirements are included.

E. General Description/Purpose - A brief (1-3 paragraph) description of the function and purpose of the system (e.g., Medicare claims processing, network support for an organization, business census data analysis, crop reporting support, etc.).

Computer security requirements should be coordinated between end users and those responsible for any support system(s) being used. Plans for such requirements must be based on an understanding of what is being protected. Thus, if this is a general support system, the nature of the uses made or the applications being supported should also be described.

F. System Environment and Special Considerations - A brief (1-3 paragraphs) general description of the technical system. Include any environmental factors that cause special security concerns, such as: it is located in a harsh or overseas environment; software is rapidly implemented; it is an open network used by the general public or with overseas access; the application is processed at a facility outside of the agency's control; the general support mainframe has dial-up lines; etc.

G. Information Contact(s) - The name, title, organization, and telephone number of one or more persons designated to be the point of contact for this system. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

II. SENSITIVITY OF INFORMATION HANDLED

This section should provide a description of the types of information handled by the system and thus provide the basis for the system's security requirements. It should contain the following information:

A. Applicable Laws or Regulations Affecting the System - List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of information in the system. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census data). Note: This should not be a list of technical standards concerning how to protect systems once the need for such protection has been determined. For this reason, the Computer Security Act of 1987 should not be listed here.

Appendix B

If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) is used for computer matching activities.

B. General Description of Information Sensitivity - The purpose of this section is to indicate the type and relative importance of protection needed for the identified system. A system may need protection for one or more of the following reasons:

- o Confidentiality - The system contains information that requires protection from unauthorized disclosure. Examples: timed dissemination (e.g., crop report data), personal data (covered by Privacy Act), proprietary business information.
- o Integrity - The system contains information which must be protected from unauthorized, unanticipated or unintentional modification, including the detection of such activities. Examples: systems critical to safety or life support, financial transaction systems.
- o Availability - The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses. Examples: air traffic control, economic indicators, or hurricane forecasting.

Describe, in general terms, the information handled by the system and the need for protective measures.

- o Relate the information handled to each of the three basic protection requirements above (confidentiality, integrity, and availability).
- o Include a statement of the estimated risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. To the extent possible, describe this impact in terms of cost, inability to carry out mandated functions, timeliness, etc.

For each of the three categories (confidentiality, integrity, and availability), indicate if the protection requirement is:

- o High - a critical concern of the system.
- o Medium - an important concern, but not necessarily paramount in the organization's priorities.
- o Low - some minimal level of security is required, but not to the same degree as the previous two categories.

III. SYSTEM SECURITY MEASURES

This section should describe the control measures (in place or planned) that are intended to meet the protection requirements of the system. The types of control measures should be consistent with the need for protection of the system described in the previous section.

A. **Risk Assessment and Management** - Risk assessment and management are crucial elements of the security planning process which include identification of informational and other assets of the system, threats that could affect the Confidentiality / integrity / availability of the system, important system vulnerabilities to the threats, potential impacts from threat activity, identification of protection requirements to control the risks, and selection of appropriate security measures. How was the risk related to the above-listed factors determined for this system?

B. **Applicable Guidance** - Indicate, to the extent practical, specific standards or other guidance used in the design, implementation, or operation of the protective measures used on the system (e.g., relevant Federal or industry standards). This should include agency policy and guidance documents.

C. **Security Control Measures** - Two sets of controls are discussed on subsequent pages - one for Major Applications and the other for General Support Systems. Controls included should be addressed from the perspective of the individual having direct management responsibility for the system. For each system, only the set corresponding to the system category designated under Basic System Identification needs to be completed.

The controls described are derived from requirements and guidance in the Computer Security Act, OMB Circular No. A-130, Appendix III, "Management of Federal Information Resources," and applicable Federal Information Processing Standards and Special Publications produced by the National Institute of Standards and Technology.

D. **Security Control Measure Status** - For each control measure on the appropriate list, specify whether it is:

- o In Place - Control measures of the type listed are in place and operational, and judged to be effective. Describe in general terms.
- o Planned - Specific control measures (new, enhanced, etc.) are planned for the system. A general description of the planned measures, resources involved and expected operational dates should be provided.

- o In Place and Planned - Some measures are in place, while others are planned. A general description of the measures in place and those planned, including the resources involved and expected operational dates should be provided.
- o Not Applicable - This type of control measure is not needed, cost-effective, or appropriate for this system. Explain.

NOTE. For operational systems, some specific controls of a given type may be "In Place," while others may be "Planned." For systems under development or undergoing a major modification, it is expected that many measures will be "Planned."

E. Security Control Measures for Major Applications

The following categories of security controls should be addressed for systems which have been identified as major application systems.

1. MANAGEMENT CONTROLS - overall management controls of the application system.

a. Assignment of Security Responsibility - Responsibility for the security of the application should be assigned.

b. Personnel Screening - Personnel security policies and procedures should be in place and working to limit access to and processing within the application system to those with a need for such access. Where appropriate, the duties of those with access should be separated. Additionally, requirements such as screening individuals with access to the application as well as those participating in the design, development, operation, or maintenance of it may be used.

2. DEVELOPMENT/IMPLEMENTATION CONTROLS - procedures to assure protection is built into the system, especially during system development.

a. Security Specifications - Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application.

b. Design Review and Testing - A design review and systems test should have been performed for this application prior to placing it into operation, to assure the application meets the security specifications. The results of the design reviews and system tests should be fully documented and maintained in the official agency records.

c. **Certification** - Prior to the application being put into operation, an agency official should certify that the application meets all applicable Federal policies, regulations, and standards, and that protection measures appear adequate. If the application has been in operation for a period of time, it should have been audited or reviewed and recertified within the last three years.

3. **OPERATIONAL CONTROLS** - day-to-day procedures and mechanisms to protect operational application systems (or planned applications when they become operational).

a. **Physical & Environmental Protection** - Physical protections in the area where processing on the application system takes place (e.g., locks on terminals, physical barriers around the processing area, etc.).

b. **Production, I/O Controls** - Controls over the proper handling, processing, storage, and disposal of input and output data and media, as well as access controls (such as labeling and distribution procedures) on the data and media.

c. **Emergency, Backup, and Contingency Planning** - Workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. They should be coordinated with the back-up and recovery plans of any installations/networks used by the application.

d. **Audit and Variance Detection** - Controls which allow management to conduct an independent review of records and activities to test the adequacy of controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such things as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles.

e. **Application Software Maintenance Controls** - Controls used to monitor the installation of and updates to application software to ensure that the software functions as expected and that an historical record is maintained of application system changes. Such controls also help to ensure that only authorized software is allowed on the system. These controls may include software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include some products used for "virus" protection.

f. **Documentation** - Controls in the form of descriptions of the hardware, software, and policies, standards, and procedures related to computer security, to include backup

and contingency activities. They also include descriptions of end user procedures. Documentation should be coordinated with the data center and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations.

4. SECURITY AWARENESS AND TRAINING - security awareness and training of users, technical staff, and managers concerning the application.

a. Security Awareness and Training Measures - All employees involved with the management, use, design, development, maintenance or operation of the application should be aware of their security responsibilities and trained how to fulfill them.

5. TECHNICAL CONTROLS - hardware and software controls used to provide automated and/or facilitate manual protections. Normally these types of controls are coordinated with the network and/or data center manager.

a. User Identification and Authentication - Controls used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information, to perform an activity, or to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Such controls include the use of passwords, tokens, biometrics or other personal mechanisms to authenticate identity.

b. Authorization/Access Controls - Hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

c. Data Integrity/Validation Controls - Controls used to protect data from accidental or malicious alteration or destruction, and provide assurance to the user that the data meets an expectation about its quality (e.g., EFT message authentication). Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

d. Audit Trails and Journaling - Controls that provide a transaction monitoring capability with a chronological record of application activities. This enables reconstruction of a transaction from its inception to final results -- including any modification of files.

6. COMPLEMENTARY CONTROLS PROVIDED BY SUPPORT SYSTEMS - The person responsible for the application should understand and

accept the risk inherent in processing on the network or at the installation(s) that support the application, particularly where the support system is operated outside of their management control (e.g. by another agency). If not, plans for greater understanding of that risk should be described.

F. Security Control Measures for General Support Systems

The following categories of security controls should be addressed for systems which have been identified as general support systems.

1. MANAGEMENT CONTROLS - overall management controls of the general support system.

a. Assignment of Security Responsibility - Responsibility for the security of each support system should be assigned to a management official knowledgeable in information technology and security matters.

b. Risk analysis - A risk analysis consists of a structured approach to identify assets, determine threats and vulnerabilities, estimate potential impacts, identify applicable controls and their costs, and select cost-effective controls for use. Include the name of any automated or formalized manual methodology used.

c. Personnel Screening - Personnel security policies and procedures should be in place and working to control access to and within the support system to assure that only those with a need for access have it. Such policies and procedures may include requirements for screening individuals involved in the operation, management, security, design, programming, or maintenance of the system.

2. ACQUISITION/DEVELOPMENT/INSTALLATION CONTROLS - procedures to assure that protection is built into the system.

a. Acquisition Specifications - Appropriate technical, administrative, physical, and personnel security requirements are to be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services.

b. Accreditation/Certification - Accreditation is management authorization and approval to process sensitive information in an operational environment. Issued by a designated official, it usually includes any constraints for processing in the environment. It is normally based on a certification, which is a technical evaluation that indicates how well a design/implementation meets a specified set of computer security requirements.

3. OPERATIONAL CONTROLS - day-to-day procedures and mechanisms to protect operational systems.

a. Physical & Environmental Protection - Controls used to protect against a wide variety of physical and environmental threats and hazards including deliberate intrusions, natural or man-made hazards, and utility outages or breakdowns (e.g., computer room locks, special fire fighting equipment, "hardened" communications, etc.).

b. Production, I/O Controls - Controls over the handling, processing, storage, and disposal of input and output from the support system (e.g., controlled or locked output boxes, tape or data screening, etc.).

c. Emergency, Backup, and Contingency Planning - Appropriate emergency, backup and contingency plans should be in place and tested regularly to assure the continuity of support in the event of system failure. These plans should be known to users and coordinated with their plans.

d. Audit and Variance Detection - Controls that allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.

e. Hardware and System Software Maintenance Controls - Controls used to monitor the installation of and updates to hardware and operating system and other system software to ensure that the software functions as expected and that an historical record is maintained of system changes. They may also be used to ensure that only authorized software is allowed on the system. These controls may include hardware and system software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include some products useful for "virus" protection.

f. Documentation - Controls in the form of descriptions of the hardware, software, and policies, standards, and procedures related to computer security on the support system, to include backup and contingency activities. They also include descriptions of operator procedures.

4. SECURITY AWARENESS AND TRAINING - security awareness and training of users, technical staff, and managers concerning the system.

a. **Security Awareness and Training Measures** - All employees who are involved with the management, use, design, acquisition, maintenance or operation of the support system should be aware of their security responsibilities and trained how to fulfill them.

5. **TECHNICAL CONTROLS** - hardware and software controls to protect the general support system from unauthorized access or misuse, to facilitate detection of security violations, and to support security requirements for associated applications.

a. **User Identification and Authentication** - Controls used to verify the identity of a station, originator, or individual prior to allowing access to the system, or specific categories of information within the system. Such controls may also be used to verify that only authorized persons are performing certain processing activities on the system. These controls include the use of passwords, tokens, or biometrics or other personal mechanism to authenticate an identity.

b. **Authorization/Access Controls** - Hardware or software features used to detect and/or permit only authorized access to or within the system (e.g., the use of access lists). Includes controls to restrict access to the operating system, limits on access to programming resources, and controls to support security policies of associated applications.

c. **Integrity Controls** - Controls used to protect the operating system, applications and information in the system from accidental or malicious alteration or destruction, and provide assurance to users that data has not been altered (e.g., Message authentication). Note. Operating system controls and system administration procedures, which are normally described in vendor supplied documentation, should be followed.

d. **Audit Trail Mechanisms** - Controls that provide a system monitoring and recording capability to retain a chronological record of system activities. Such controls normally enable the reconstruction of system activity. The use of system log files is an example of this type of control.

e. **Confidentiality Controls** - These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. The controls may provide data protection at the user site, at a computer facility, in transit, or some combination of these (e.g., encryption).

6. CONTROLS OVER THE SECURITY OF APPLICATIONS - The security of each application that processes on a support system affects the security of all others processing there. Thus the manager of the support system should understand the risk that each application represents to the system. If not, plans for greater understanding of that risk should be described. (e.g., Application users that have access to programming capability represent a higher risk to the support system than when they are confined to individual application functions. Similarly, applications that utilize dial-up communications represent a higher risk.)

IV. ADDITIONAL COMMENTS

This final section is intended to provide an opportunity to include additional comments about the security of the subject system and any perceived need for guidance or standards.